CARE
Cyber Asset Recovery Experts

CRYPTOCURRENCY TRACING REPORT

David Gonzalez

Abstract

CARE has traced additional funds stolen after May 8, 2021 and conducted analysis of the opportunity cost lost due to the theft.

Jason T. Ghetian
support@cyberassetrecovery.com
https://cyberassetrecovery.com

Table of Contents

I. EXECUTIVE SUMMARY

1.1 At the request of the client, I was tasked to Trace the remainder of ERC-20 Tokens and Ethereum stolen from Mr. Gonzalez after 5/8/2021. The stolen funds were laundered primarily through asset hops, using Decentralized Exchanges such as Uniswap, 1inch, SushiSwap, 0x Exchange Protocol, and Aggregation Router 5, before being sent to the following Virtual Asset Service Providers (aka "Exchanges"):

BITREFILL BINANCE REMITANO CRYPTO.COM

1.2 Some of the stolen funds were sent to crypto addresses and have remained for years, most likely due to their extremely low value.

1.3 The unknown individual who hacked Mr. Gonzalez's account went dormant in November 2021 but reappeared in Mr. Gonzalez's wallet in August 2024 to liquidate a few more ERC-20 tokens that had little to no value. The transactions in 2024 appears to have been conducted by the same individual due to the use of the same crypto addresses used on 5/8/2021 to steal Mr. Gonzalez's funds.

1.5 An analysis was conducted of the opportunity cost lost to Mr. Gonzalez from the theft of his cryptocurrency. Based on my analysis, Mr. Gonzalez lost the opportunity to make trillions of dollars, primarily from the theft of his Hokkaidu Inu Tokens (HOKK). An unknown individual stole 90,934,964,476,560 HOKK from Mr. Gonzalez's wallet which, at the time of the transaction, were worth $657,205. However, the price of HOKK soared six months later in November 2021 rising from 0.000000001250660960331 87 per HOKK to a peak of 0.03727 per HOKK on 11/15/2021. If Mr. Gonzalez could have sold his HOKK on 11/15/2021 for the peak value, he would have made $3,389,146,126,041. Even if Mr. Gonzalez missed the peak of HOKK's value by as much as a month, the price of HOKK was still as high as .004337 on 1/16/2022 which would have made Mr. Gonzalez's HOKK worth **$401,603,146,222**.

II. BACKGROUND OF JASON T. GHETIAN

2.1 I am the Owner and President of Cyber Asset Recovery Experts, Inc ("CARE"), opened in December 2023 after retiring from the Federal Bureau of Investigation ("FBI") after serving twenty years as a Special Agent ("SA"). At CARE, I conduct cryptocurrency traces for victims of cryptocurrency cyber-crimes.

2.2 Prior to my retirement, I was assigned to the Orange County Resident Agency ("OCRA") of the FBI's Los Angeles Field Office. At OCRA, I investigated cyber-related crimes in and around Orange County, California, including cyber-enabled fraud and cryptocurrency scam cases, including the largest cryptocurrency crime in the world, the Pig Butchering Scam. I am also the founder of the Orange County Cyber Task Force (OCCTF) made up of Investigators and Analysts from the Internal Revenue Service, Homeland Security, Federal Deposit Insurance Corporation Office of Inspector General, Orange County Intelligence Assessment Center, and other state and local law enforcement agencies.

2.3 In 2023, I was nominated by the Department of Justice's National Cryptocurrency Enforcement Team (NCET) for the Attorney General's Award for leading the U.S. Government's efforts on Pig Butchering. I have also received four United States Attorney's Awards for my investigations.

2.4 I am a graduate of the United States Military Academy with a degree in Mechanical Engineering and the University of Southern California with a Master of Cyber Security.

2.5 I have also obtained numerous other cyber-related certifications including my Certified Information Systems Security Professional (CISSP)[1] and the following from The SANS Institute[2]: GIAC Information Security Professional (GISP); GIAC Certified Forensic Examiner (GCFE); GIAC Certified Incident Handler (GCIH); and GIAC Information Security Fundamentals (GISF).

2.6 During my career as an FBI SA, I have received both formal and informal training from the FBI and other institutions regarding computer-related investigations, computer technology, and cryptocurrency tracing. I have received training in investigations of computer and high-technology crimes, including computer intrusions, access-device fraud, denial of service attacks, and other types of malicious computer activity. I also obtained my FBI Digital Evidence Extraction Technician (DeXT) and Computer Analysis Response Team (CART) certifications.

2.7 In addition, I have received extensive training in cryptocurrency tracing, both formal and informal, including Cryptocurrency Tracing using Chainalysis and the Advanced Cryptocurrency Course offered by the California Department of Justice. I also possess the following TRM certifications: TRM Cryptocurrency Fundamentals; TRM Certified Investigator; and TRM Advanced Certified Investigator.

III. INITIAL TRANSACTIONS

3.1 List of Initial Transactions

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Asset
5/8/21 1:25:23 PM	***Tx Hash 33***	A1	0x95f0d3169e8734f300a91bce591f543f246485fa	0.151266183	ETH
5/8/21 3:55:19 PM	***Tx Hash 34***	A1	0x95f0d3169e8734f300a91bce591f543f246485fa	0.072869346	ETH
5/17/21 1:39:18 PM	***Tx Hash 39***	J1	0x3e9cf220b4e78f016b85bf28548bc0d2f66765cd	0.010867153	ETH
5/22/21 12:24:00 PM	***Tx Hash 42***	Uniswap	0xdfc14d2af169b0d36c4eff567ada9b2e0cae044f	0.553093036	AAVE
6/1/21 12:19:41 PM	***Tx Hash 52***	S1	0x0000000000000000000000000000000000000000	15	stkAAVE
6/2/21 10:58:48 AM	***Tx Hash 58***	M2	0x3b9a8ca54ee22d03a3239758a2c3b447e6d6c5b2	206.4917824	FTM
6/2/21 11:02:06 AM	***Tx Hash 59***	M2	0x3b9a8ca54ee22d03a3239758a2c3b447e6d6c5b2	14.058493	SRM

[1] The Certified Information Systems Security Professional (CISSP) is an information security certification for security analysts. It was created by the International Information Systems Security Certification Consortium (ISC). The certification was created to ensure professionals in computer security have standardized knowledge of the field.

[2] The SANS Institute is a private U.S. for-profit company founded in 1989 that specializes in information security, cybersecurity training, and selling certificates. Topics available for training include cyber and network defenses, penetration testing, incident response, digital forensics, and auditing.

6/2/21 11:02:18 AM	***Tx Hash 60***	M2	0x3b9a8ca54ee22d03a3239758a2c3b447e6d6c5b2	34.5149981	SXP
6/2/21 11:11:44 AM	***Tx Hash 62***	M2	0x3b9a8ca54ee22d03a3239758a2c3b447e6d6c5b2	3,790.22	MXC
6/2/21 11:11:44 AM	***Tx Hash 63***	J1	0x3e9cf220b4e78f016b85bf28548bc0d2f66765cd	611.2925109	AERGO
6/2/21 10:58:00 AM	***Tx Hash 56***	LID	0x9a54fe35d41bc7c8f7071abf0ccd952505e29ceb	49.74667418	LID
6/2/21 11:12:50 AM	***Tx Hash 67***	M2	0x3b9a8ca54ee22d03a3239758a2c3b447e6d6c5b2	3,127.37	AKRO
6/2/21 11:24:19 AM	***Tx Hash 68***	M1	0xb646ba2ce3f23fbc9db142a2e0fb515d07d029d7	159.0604363	CVR
7/1/21 3:13:28 PM	***Tx Hash 70***	Uniswap	0x05f21e62952566cefb77f5153ec6b83c14fb6b1d	746.0104865	RFuel
7/1/21 3:26:13 PM	***Tx Hash 71***	A1	0x95f0d3169e8734f300a91bce591f543f246485fa	29.878423	USDT
8/21/21 6:51:17 AM	***Tx Hash 74***	Uniswap	0xb773a5a7ee006d2675537588e3233ad37be53bb9	139.9968407	C3
8/31/21 4:07:56 PM	***Tx Hash 84***	J1	0x3e9cf220b4e78f016b85bf28548bc0d2f66765cd	0.010212997	ETH
9/1/21 4:21:51 AM	***Tx Hash 85***	S1	0x69c707d975e8d883920003cc357e556a4732cd03	2.097088785	STAKE
9/19/21 11:25:26 AM	***Tx Hash 86***	Uniswap	0x1e0693f129d05e5857a642245185ee1fca6a5096	40.31788903	AXIAv3
9/19/21 11:29:03 AM	***Tx Hash 87***	Uniswap	0xb27de0ba2abfbfdf15667a939f041b52118af5ba	21.78691028	UBT
11/8/21 4:47:32 PM	***Tx Hash 90***	U1	0x4358bddd848d533f6a17a13cad61a70c090d39db	0.007041599	ETH
8/4/24 12:12:47 AM	***Tx Hash 93***	0x Exch	0x22f9dcf4647084d6c31b2765f6910cd85c178c18	1.192594883	YFBETA
8/4/24 12:13:59 AM	***Tx Hash 94***	0x Exch	0x22f9dcf4647084d6c31b2765f6910cd85c178c18	81.06164319	SWFL
8/4/24 12:15:23 AM	***Tx Hash 95***	Agg Exch	0xe37e799d5077682fa0a244d46e5649f71457bd09	1,832.24	XAMP
8/4/24 12:16:59 AM	***Tx Hash 96***	0x Exch	0x22f9dcf4647084d6c31b2765f6910cd85c178c18	156.192684	FRM
8/22/24 1:07:35 PM	***Tx Hash 105***	W3	0x829c23f7df91897f82edda60186abce9cbd191e6	0.002986644	ETH
8/22/24 1:09:47 PM	***Tx Hash 108***	W3	0x829c23f7df91897f82edda60186abce9cbd191e6	0.0029496	ETH
8/22/24 1:25:23 PM	***Tx Hash 113***	W2	0x75b4cac515db8b4c154b77ff2da0778c1441f766	0.002802056	ETH
8/22/24 2:19:59 PM	***Tx Hash 116***	W5	0x792194dad565197d3cabdebb612f66f05fc346f0	0.002252102	ETH
8/22/24 3:24:23 PM	***Tx Hash 121***	W2	0x75b4cac515db8b4c154b77ff2da0778c1441f766	0.002315676	ETH
8/29/24 3:39:11 PM	***Tx Hash 125***	W2	0x75b4cac515db8b4c154b77ff2da0778c1441f766	426.101647	SWAP
8/29/24 3:39:59 PM	***Tx Hash 126***	W2	0x75b4cac515db8b4c154b77ff2da0778c1441f766	0.000783083	ETH
8/30/24 8:38:35 AM	***Tx Hash 130***	W2	0x75b4cac515db8b4c154b77ff2da0778c1441f766	0.003737219	ETH

Total value in USD: $8,211.66

III. SUMMARY OF FUND DESTINATIONS

4.1 VASP Wallets

The law regarding cryptocurrency is still unsettled in the United States. Some jurisdictions within the United States allow a victim to seize all the funds in a given VASP wallet due to the comingling of criminal funds with non-criminal funds; Other jurisdictions do not allow this. During the trace, CARE employees are careful in determining the exact portions of funds from the original victim payments are identified in each outgoing VASP (found in the column labeled 'PIFO.') The conservative rule of thumb is a victim can only seize the funds in a given VASP wallet that can be directly tied to the initial criminal transaction. This is the rule being used by FBI Crypto Tracers despite there being no clear policy on the matter within the FBI.

4.2 VASP Table

Hash Label	Sending Wallet	Receiving Wallet	VASP	Amount	Asset	PIFO	Trace
48	0xe2d3798d4daf200999d5074d0c38797c8af730bf	0x4945ce2d1b5bd904cac839b7fdabafd19cab982b	Bitrefill	0.546017	ETH	0.012542	K
51	0xea9fd7e15c48a5d853f4bc422456f6e1c8bf7a1a	0x2819c144d5946404c0516b6f817a960db37d4929	Remitano	0.1272916	ETH	0.034919203	K
55	0xcbf7ec8a9d0ac78434389f1473a92d9b9a14fecb	0x28c6c06298d514db089934071355e5743bf21d60	Binance	2.2241616	ETH	2.148919347	L
59	0x3b9a8ca54ee22d03a3239758a2c3b447e6d6c5b2	0x28c6c06298d514db089934071355e5743bf21d60	Binance	34.514998	SXP	34.5149981	M
64	0x4d9d8614908077d1765dbc4482ee47c8078295d11	0x2819c144d5946404c0516b6f817a960db37d4929	Remitano	0.0817778	ETH	0.042905198	N
71	0x19456d9b965026ab3fb1086e9236e342b9fc399a	0x28c6c06298d514db089934071355e5743bf21d60	Binance	108.01210	USDT	25	P
79	0xfc039f8687caf47f79e5034f3231b197633bf648	0x6262998ced04146fa42253a5c0af90ca02dfd2a3	Crypto	0.0644800	ETH	0.014875975	Q
81	0xea9fd7e15c48a5d853f4bc422456f6e1c8bf7a1a	0x2819c144d5946404c0516b6f817a960db37d4929	Remitano	0.3738177	ETH	0.148546809	Q
83	0x0e6ec53eb9742b98a865571bd25e3c6daa4c8dac	0x69c707d975e8d883920003cc357e556a4732cd03	Stake	2.0970888	STAKE	2.097088785	S
87	0x003a2d9ad66dda7cc85622bdf298f043cf66088c	0x2819c144d5946404c0516b6f817a960db37d4929	Remitano	0.0539578	ETH	0.053957803	T
99	0x93043043974add793766edd2e6b92caabfddd5fe	0xb8356a14e2610315f4d6604c71738c7f2ef7aa2a	Remitano	0.0239919	ETH	0.001240646	V

111	0x93043043974ad d793766edd2e6b9 2caabfddd5fe	0xb8356a14e2610 315f4d6604c7173 8c7f2ef7aa2a	Remitano	0.0117728	ETH	0.01177284	W
129	0x93043043974ad d793766edd2e6b9 2caabfddd5fe	0xb8356a14e2610 315f4d6604c7173 8c7f2ef7aa2a	Remitano	0.0173722	ETH	0.017372213	X

4.3 Wallets Containing Stolen Funds

Wallet Label	Receiving Wallet	Amount	Asset	PIFO	Trace	Wallet Value
M2	0x3b9a8ca54ee22d03a3239758a2 c3b447e6d6c5b2	206.49178	FTM	206.49178	M	$83.75
M2	0x3b9a8ca54ee22d03a3239758a2 c3b447e6d6c5b2	14.058493	SRM	14.058493	M	$0.41
M2	0x3b9a8ca54ee22d03a3239758a2 c3b447e6d6c5b2	3,790.22	MXC	3,790.22	M	$25.22
M2	0x3b9a8ca54ee22d03a3239758a2 c3b447e6d6c5b2	3,127.37	AKRO	3,127.37	M	$13.10
W4	0x53f001dfc26792599363139888 1efd5befeb9ac4	0.0029012	ETH	0.0029012	W	$6.57
X1	0x4ab7849af9fabd73208a531c036 c69b9d5ca4e43	0.0046624	ETH	0.0046624	X	$78.65

V. TRACE I

I.1 Transaction 1 & 2 – Ethereum stolen from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
5/8/21 1:25:23 PM	***Tx Hash 33***	A1	0x95f0d3169e8734f300a91bc e591f543f246485fa	0.151266183	ETH
5/8/21 3:55:19 PM	***Tx Hash 34***	A1	0x95f0d3169e8734f300a91bc e591f543f246485fa	0.072869346	ETH

Note: All transactions on the Ethereum Blockchain include Transaction Fees, aka "Gas Fees," pulled from the associated ETH funds contained within the account. Without ETH, the address cannot make transactions, including ERC-20 transactions. Transaction Hash 33 was the first ETH transaction into A1 which provided the initial gas to conduct further transactions using A1.

I.2 Transaction 3

The third transaction occurred on 5/8/2021 at 4:16:06 PM where 0.0536725485467713 ETH was transferred from A1 to 0x35e4c02fce6571c34514d626968ea116e9063bcb ("B2"). ***Tx Hash 35***.

I.3 Transaction 4

The fourth transaction occurred on 5/8/2021 at 4:18:52 PM where 0.0600025406162474 ETH was also transferred from A1 to B2. ***Tx Hash 36***.

I.4 Transaction 5

The fifth transaction occurred on 5/8/2021 at 4:23:27 PM where 0.13358 ETH was transferred from B2 back to A1. ***Tx Hash 37***.

I.5 Transaction 6

The sixth transaction occurred on 5/8/2021 at 5:17:31 PM where 0.0393127356454414 ETH was transferred from A1 back to A2. ***Tx Hash 38***.

I.6 Explanation

The unknown cyber actor stole ETH from Mr. Gonzalez to pay for the Transaction Fees for A1 and B2 to steal other ERC-20 assets from Mr. Gonzalez as described in my previous report.

VI. TRACE J

J.1 Transaction 1 - Ethereum stolen from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
5/17/21 1:39:18 PM	***Tx Hash 39***	J1	0x3e9cf220b4e78f016b85 bf28548bc0d2f66765cd	0.010867153	ETH

I.2 Transaction 2

The second transaction occurred on 5/18/2021 at 7:17:35 PM where 0.014777 ETH was transferred from J1 to 0xf49c41ab9a27e70b416fbaa1edf4819f71dd3a10 ("J2"). ***Tx Hash 40***.

I.3 Transaction 3

The third transaction occurred on 5/1/2022 at 9:49:00 AM where 0.014147 ETH was transferred from J2 to 0x50cb18bc258b244817abc295578e46d598e16166 ("J3"). ***Tx Hash 41***. J3 has 3,113 transactions so it appears the cyber actor transferred the value to a 3rd party or conducted additional money laundering techniques using an Unattributable Exchange ("DEX"). Further, the value of the ETH was a mere $39.98 so the trace was discontinued.

VII. TRACE K

K.1 Transaction 1 - **Aave** Tokens stolen from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
5/22/21 12:24:00 PM	***Tx Hash 42***	UNISWAP V2	0xdfc14d2af169b0d36c4eff567ada9b2e0cae044f	0.553093036	AAVE

The first transaction occurred on 5/22/2021 at 12:24:00 PM where 0.553093036 AAVE was converted to 0.079942552 ETH using Uniswap V2 and returned to the Victim's Wallet.

K.2 Transaction 2

The second transaction occurred on 5/22/2021 at 12:28:00 PM where 0.118883461 ETH was transferred from The Victim's Wallet to A1. ***Tx Hash 43***. The funds were then split into four separate transactions: K.3, K.6, K.8, and K.9.

K.3 Transaction 3

The third transaction occurred on 5/28/2021 at 1:42:00 PM where 0.005391696 ETH was transferred from Wallet A1 to 0xb374161a6c141dd3d1414c1ffc1c0766c795f4d6 ("K1"). ***Tx Hash 44***.

K.4 Transaction 4

The fourth transaction occurred on 6/1/2021 at 11:59:00 AM where 0.002962778 ETH was transferred from K1 to A1. ***Tx Hash 45***. The rest of the funds were used for transactions fees for K1.

K.5 Transaction 5

The fifth transaction occurred on 5/28/2021 at 2:01:00 PM where 0.047616898 ETH was transferred from A1 back to the Victim's Wallet to pay for Transaction Fees. ***Tx Hash 46***.

K.6 Transaction 6

Returning to the split referenced in Transaction K.2, the sixth transaction occurred on 6/8/2021 at 4:48:00 PM where 0.012542 ETH was transferred from A1 to 0xe2d3798d4daf200999d5074d0c38797c8af730bf ("K2"), which is potentially a BITREFILL account holder address. ***Tx Hash 47***.

K.7 Transaction 7

The seventh transaction occurred on 6/10/2021 at 10:05:00 PM where 0.546017 ETH was transferred from K2 to 0x4945ce2d1b5bd904cac839b7fdabafd19cab982b ("K3"), which is a BITREFILL Hot Wallet. ***Tx Hash 48***.

K.8 Transaction 8

Returning to the split referenced in Transaction K.2, the eighth transaction occurred on 7/1/2021 at 2:48:00 PM where 0.008622096 ETH was transferred from A1 back to The Victim's Wallet in order to pay for Transaction Fees. ***Tx Hash 49***.

K.9 Transaction 9

The ninth transaction was the last of the split referenced in Transaction K.2 which occurred on 7/4/2021 at 8:01:00 AM where 0.12834155 ETH was transferred from A1 to 0xea9fd7e15c48a5d853f4bc422456f6e1c8bf7a1a ("K4"), which is potentially a REMITANO account holder address. ***Tx Hash 50***.

K.10 Transaction 10

The tenth transaction occurred on 7/4/2021 at 8:05:00 AM where 0.12729155 ETH was transferred from K4 to 0x2819c144d5946404c0516b6f817a960db37d4929 ("K5"), which is a REMITANO Hot Wallet. ***Tx Hash 51***.

VIII. TRACE L

L.1 Transaction 1 – Staked **Aave Tokens** stolen from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
6/1/21 12:19:41 PM	***Tx Hash 52***	STAKE	0x0000000000000000000000000000000000000000	15	stkAAVE

The first transaction occurred on 6/1/2021 at 12:19:41 PM where a "redeem call" was made for 15 stkAAVE resulting in 15 AAVE being transferred to the Victim's Wallet.

L.2 Transaction 2

The second transaction occurred on 6/1/2021 at 12:22:43 PM where 15 AAVE was converted to 2.14891934714188 ETH using Uniswap V2 and returned to the Victim's Wallet. ***Tx Hash 53***.

L.3 Transaction 3

The third transaction occurred on 6/1/2021 at 12:23:43 PM where 2.18691256786773 ETH was transferred to 0xcbf7ec8a9d0ac78434389f1473a92d9b9a14fecb ("B3"), belonging to a BINANCE account holder. ***Tx Hash 54***. This account holder is also the recipient of 144.860726702924 ETH stolen from Mr. Gonzalez.

L.4 Transaction 4

The fourth transaction occurred on 6/1/2021 at 5:21:30 PM where 2.22416156786773 ETH was transferred to 0x28c6c06298d514db089934071355e5743bf21d60 ("L1"), a BINANCE Hot Wallet. ***Tx Hash 55***.

IX. TRACE M

M.1 Transaction 1 – **Liquidity Dividends Protocol**, **Fantom**, **Serum**, **Swipe**, **MXC**, and **Akropolis** Tokens stolen from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
6/2/21 10:58:00 AM	***Tx Hash 56***	LID	0x9a54fe35d41bc7c8f7071abf0ccd952505e29ceb	49.74667418	LID
6/2/21 10:58:48 AM	***Tx Hash 58***	M2	0x3b9a8ca54ee22d03a3239758a2c3b447e6d6c5b2	206.4917824	FTM
6/2/21 11:02:06 AM	***Tx Hash 59***	M2	0x3b9a8ca54ee22d03a3239758a2c3b447e6d6c5b2	14.058493	SRM
6/2/21 11:02:18 AM	***Tx Hash 60***	M2	0x3b9a8ca54ee22d03a3239758a2c3b447e6d6c5b2	34.5149981	SXP
6/2/21 11:11:44 AM	***Tx Hash 62***	M2	0x3b9a8ca54ee22d03a3239758a2c3b447e6d6c5b2	3,790.22	MXC
6/2/21 11:12:50 AM	***Tx Hash 67***	M2	0x3b9a8ca54ee22d03a3239758a2c3b447e6d6c5b2	3,127.37	AKRO

On 6/2/2021 at 10:58:20 AM, 2,618.25 LID was transferred from the Victim's Wallet and after Transaction Fees, 2,565.88108947357 LID arrived at 0xb646ba2ce3f23fbc9db142a2e0fb515d07d029d7 ("M1"). The FTM, SRM, MXC, and AKRO Tokens stolen from Mr. Gonzalez were transferred to M2 where they still remain. However, the present day value of the tokens are only $175.91.

M.2 Transaction 2

The second transaction occurred on 6/2/2021 at 2:33:48 PM where 2,565.88108947357 LID was converted to 0.00190168459713178 ETH, using Uniswap V2 and 1inchV2, and returned to M1. ***Tx Hash 57***. The value of the ETH was worth approximately $5.16 so the trace was discontinued.

M.3 Transaction 3

The third transaction occurred on 5/19/2023 at 3:30:35 AM where 15.15 SXP was transferred to L1, a BINANCE Hot Wallet. ***Tx Hash 61***.

X. TRACE N

N.1 Transaction 1 – **Aergo** Tokens stolen from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
6/2/21 11:11:44 AM	***Tx Hash 63***	J1	0x3e9cf220b4e78f016b85bf28548bc0d2f66765cd	611.29251	AERGO

N.2 Transaction 2

The second transaction occurred on 11/7/2021 at 7:53:20 PM where 611.29251086567 AERGO was converted to 0.0429051976740831 ETH using SushiSwap and returned to Wallet J1. ***Tx Hash 64.***

N.3 Transaction 3

The third transaction occurred on 11/7/2021 at 9:53:46 PM where 0.0863462040778761 ETH was transferred from J1 to 0x4d9d861490807d1765dbc4482ee47c8078295d11 ("N1"), which is potentially a REMITANO account holder address. ***Tx Hash 65***.

N.4 Transaction 4

The fourth transaction occurred on 11/7/2021 at 9:58:08 PM where 0.0817778194588401 ETH was transferred from N1 to K5, which is a REMITANO Hot Wallet. ***Tx Hash 66***.

XI. TRACE O

O.1 Transaction 1 – **PolkaCover** Tokens converted to Ethereum and used for Victim Wallet's Transaction Fees

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
6/2/21 11:24:19 AM	***Tx Hash 68***	M1	0xb646ba2ce3f23fbc9db142a2e0fb515d07d029d7	159.0604363	CVR

O.2 Transaction 2

The second transaction occurred on 6/2/2021 at 12:19:56 PM where 159.060436315435 CVR was converted to 0.0176121331046164 ETH using Uniswap V2 and returned to Wallet M1 and used for Transaction Fees. ***Tx Hash 69.***

XI. TRACE P

P.1 Transaction 1 – **Rfuel** Tokens stolen from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
7/1/21 3:13:28 PM	***Tx Hash 70***	Uniswap	0x05f21e62952566cefb77f5153ec6b83c14fb6b1d	746.0104865	RFuel

The first transaction occurred on 7/1/2021 at 3:13:28 PM where 746.010486472624 RFuel was converted to 29.878423 USDT using Uniswap V2 and returned to the Victim's Wallet.

P.2 Transaction 2

The second transaction occurred on 7/1/2021 at 3:26:13 PM where 29.878423 USDT was transferred from the Victim's Wallet to A1. ***Tx Hash 71***.

P.3 Transaction 3

The third transaction occurred on 7/15/2021 at 12:54:01 PM where 25 ISDT was transferred to 0x19456d9b965026ab3fb1086e9236e342b9fc399a ("P1"), believed to be a BINANCE account holder. ***Tx Hash 72***.

L.4 Transaction 4

The fourth transaction occurred on 12/10/2022 at 5:52:11 PM where 108.012103 USDT was transferred to L1, a BINANCE Hot Wallet. ***Tx Hash 73***.

XII. TRACE Q

Q.1 Transaction 1 – **C3** Tokens stolen from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
8/21/21 6:51:17 AM	***Tx Hash 74***	UNISWAP V3	0xb773a5a7ee006d2675537588e3233ad37be53bb9	139.9968407	C3

The first transaction occurred on 8/21/2021 at 6:51:17 AM where 139.996840673394 C3 was converted to 0.157526596325962 ETH using Uniswap V3 and returned to the Victim's Wallet.

Q.2 Transaction 2

The second tFransaction occurred on 8/21/2021 at 6:53:06 AM where 0.163422784644334 ETH was transferred from the Victim's Wallet to A1. ***Tx Hash 75***. The funds were then split into four separate transactions: Q.3, Q.4, K.8, and K.9.

Q.3 Transaction 3

The third transaction occurred on 8/21/2021 at 8:26:21 AM where 0.00272870402415866 ETH was transferred from A1 to 0x95f0d3169e8734f300a91bce591f543f246485fa ("Q1"). ***Tx Hash 76***.

Q.4 Transaction 4

The fourth transaction occurred on 8/21/2021 at 8:26:21 AM where 0.004547823580335 ETH was transferred from A1 to Q1 where the funds were comingled with Transaction Q.3. ***Tx Hash 77***.

Q.5 Transaction 5

The fifth transaction occurred on 8/21/2021 at 8:29:29 AM where 0.010150706890397 ETH was transferred from Q1 to 0xfc039f8687caf47f79e5034f3231b197633bf648 ("Q2"), which is potentially a CRYPTO.COM account holder address. ***Tx Hash 78***

Q.6 Transaction 6

Returning to the split referenced in Transaction Q.2, the sixth transaction occurred on 8/21/2021 at 8:44:45 AM where 0.00759944787507673 ETH was transferred from A1 to Q1. ***Tx Hash 79***.

Q.7 Transaction 7

The seventh transaction occurred on 8/21/2021 at 8:45:23 AM where 0.0499062282430796 ETH was transferred from Q1 to Q2 and comingled with the funds from Q.5. ***Tx Hash 80***.

Q.8 Transaction 8

The eighth transaction occurred on 8/4/2022 at 9:23:24 AM, almost a year later, where 0.0644800206487117 ETH was transferred from Q2 to 0x6262998ced04146fa42253a5c0af90ca02dfd2a3 ("Q3"), which is a CRYPTO.COM Hot Wallet. ***Tx Hash 81***.

Q.9 Transaction 9

Returning to the split referenced in Transaction Q.2, the ninth transaction occurred on 8/21/2021 at 11:52:52 AM where 0.374481453577025 ETH was transferred from A1 to K4, which is potentially a REMITANO account holder address. ***Tx Hash 82***.

Q.10 Transaction 10

The tenth transaction occurred on 8/21/2021 at 11:57:04 AM where 0.373817675818199 ETH was transferred from K4 to K5, which is a REMITANO Hot Wallet. ***Tx Hash 83***.

XII. TRACE R

Q.1 Transaction 1 – Ethereum stolen from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
8/31/21 4:07:56 PM	***Tx Hash 84***	J1	0x3e9cf220b4e78f016b85bf28548 bc0d2f66765cd	0.010212997	ETH

The ETH sent from to J1 was used to pay for Transaction Fees for J1.

XII. TRACE S

Q.1 Transaction 1 – STAKE Tokens stolen from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
9/1/21 4:21:51 AM	***Tx Hash 85***	S1	0x69c707d975e8d883920003cc35 7e556a4732cd03	2.097088785	STAKE

J3 has 1,550 Ethereum and 2,818 ERC-20 transactions so it appears the cyber actor transferred the value to a 3rd party or conducted additional money laundering techniques using an Unattributable Exchange ("DEX"). Further, the value of the STAKE was a mere $19.96 so the trace was discontinued.

XII. TRACE T

T.1 Transaction 1 – **Axia** and **UniBright** Tokens stolen from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
9/19/21 11:25:26 AM	***Tx Hash 86***	Uniswap	0x1e0693f129d05e5857a6422451 85ee1fca6a5096	40.31788903	AXIAv3
9/19/21 11:29:03 AM	***Tx Hash 87***	Uniswap	0xb27de0ba2abfbfdf15667a939f0 41b52118af5ba	21.78691028	UBT

The first transaction occurred on 9/19/2021 at 11:25:26 AM where 40.317889027807 AXIAv3 was converted to 0.0438341565650222 ETH using Uniswap V2 and returned to the Victim's Wallet. ***Tx Hash 86.***

T.2 Transaction 2

The second transaction occurred on 9/19/2021 at 11:25:26 AM where 21.78691028 UBT was converted to 0.0218234729679365 ETH using Uniswap V2 and returned to the Victim's Wallet and comingled with the funds from Transaction T.1. ***Tx Hash 87.***

T.3 Transaction 3

The third transaction occurred on 9/19/2021 at 11:32:45 AM where 0.0571336058300312 ETH was transferred from the Victim's Wallet to 0x003a2d9ad66dda7cc85622bdf298f043cf66088c ("T1"), which is potentially a REMITANO account holder address. ***Tx Hash 88***.

T.10 Transaction 4

The fourth transaction occurred on 9/19/2021 at 11:38:43 AM where 0.0539578033319042 ETH was transferred from T1 to K5, which is a REMITANO Hot Wallet. ***Tx Hash 89***.

XII. TRACE U

U.1 Transaction 1 – Ethereum stolen from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
11/8/21 4:47:32 PM	***Tx Hash 90***	U1	0x4358bddd848d533f6a17a13cad61a70c090d39db	0.007041599	ETH

U.2 Transaction 2

The second transaction occurred on 11/13/2021 at 4:36:28 PM where 0.00431159852102489 ETH was transferred from the U1 to J1. ***Tx Hash 91***.

U.3 Transaction 3

The third transaction occurred on 11/13/2021 at 10:09:10 PM where 0.015275703325727 ETH was transferred from J1 to 0x5ec0e1f904656c640ce0d9bbfb6ebca307131907 ("U2") and used for transactions fees for U2. ***Tx Hash 92***.

XII. TRACE V

V.1 Transaction 1 – **yfBETA**, **Swapfolio**, **Antiample**, **Ferrum** Tokens stolen from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
8/4/24 12:12:47 AM	***Tx Hash 93***	0x Exchange	0x22f9dcf4647084d6c31b2765f6910cd85c178c18	1.192594883	YFBETA
8/4/24 12:13:59 AM	***Tx Hash 94***	0x Exchange	0x22f9dcf4647084d6c31b2765f6910cd85c178c18	81.06164319	SWFL
8/4/24 12:15:23 AM	***Tx Hash 95***	Aggregation	0xe37e799d5077682fa0a244d46e5649f71457bd09	1,832.24	XAMP
8/4/24 12:16:59 AM	***Tx Hash 96***	0x Exchange	0x22f9dcf4647084d6c31b2765f6910cd85c178c18	156.192684	FRM

The first transaction occurred on 8/4/2024 at 12:12:47 AM where 1.19259488265427 YFBETA was converted to 0.00246830468655805 ETH using 0x: Exchange Proxy and returned to the Victim's Wallet and used for gas fees. ***Tx Hash 93.***

V.2 Transaction 2

The second transaction occurred on 8/4/2024 at 12:13:59 AM where 81.0616431881488 SWFL was converted to 0.00197949424194113 ETH using 0x: Exchange Proxy and returned to the Victim's Wallet and used for gas fees. ***Tx Hash 94.***

V.3 Transaction 3

The third transaction occurred on 8/4/2024 at 12:15:23 AM where 1,832.23606508 XAMP was converted to 0.00145560400166084 ETH using Aggregation Router 5 and returned to the Victim's Wallet and used for gas fees. ***Tx Hash 95.***

V.4 Transaction 4

The fourth transaction occurred on 8/4/2024 at 12:16:59 AM where 156.192684 FRM was converted to 0.00124064595870948 ETH using 0x: Exchange Proxy and returned to the Victim's Wallet. ***Tx Hash 96.***

V.5 Transaction 5

The fifth transaction occurred on 8/4/2024 at 12:18:11 AM where 0.00810507440587562 ETH was transferred from the Victim's Wallet to A1. ***Tx Hash 97.***

V.6 Transaction 6

The sixth transaction occurred on 8/4/2024 at 12:18:59 AM where 0.0240691681506444 ETH was transferred from the A1 to 0x93043043974add793766edd2e6b92caabfddd5fe ("V1"), which is potentially a REMITANO account holder address. ***Tx Hash 98.***

V.7 Transaction 7

The seventh transaction occurred on 8/4/2024 at 12:30:59 AM where 0.0239918663382384 ETH was transferred from V1 to 0xb8356a14e2610315f4d6604c71738c7f2ef7aa2a ("V2"), which is a REMITANO Hot Wallet. ***Tx Hash 99***.

XII. TRACE W

W.1 Transaction 1 – Attempted theft of **KardiaChain** and **Curve.fi** Tokens from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
8/22/24 1:07:35 PM	***Tx Hash 105***	W3	0x829c23f7df91897f82edda6018 6abce9cbd191e6	0.002986644	ETH
8/22/24 1:09:47 PM	***Tx Hash 107***	W3	0x829c23f7df91897f82edda6018 6abce9cbd191e6	0.0029496	ETH
8/22/24 1:25:23 PM	***Tx Hash 113***	W2	0x75b4cac515db8b4c154b77ff2d a0778c1441f766	0.002802056	ETH
8/22/24 2:19:59 PM	***Tx Hash 116***	W5	0x792194dad565197d3cabdebb6 12f66f05fc346f0	0.002252102	ETH
8/22/24 3:24:23 PM	***Tx Hash 121***	W2	0x75b4cac515db8b4c154b77ff2d a0778c1441f766	0.002315676	ETH

Prior to the thefts above, along with the attempted theft of Mr. Gonzalez's KardiaChain Tokens, the Victim's Wallet needed to be infused with Etherium in order to conduct transactions. Those funds came from 0x0189b5eac202d674b34d5407e443d94d354c59bf ("W1").

On 8/22/2024 at 12:56:11 PM, 0.01 ETH was transferred from W1 to the Victim's Wallet. ***Tx Hash 100***. At 12:57:35 PM, 0.0099540527563129 ETH was transferred from the Victim's Wallet to 0x75b4cac515db8b4c154b77ff2da0778c1441f766 ("W2"). ***Tx Hash 101.*** At 12:58:35 PM, another 0.002 ETH was transferred from W1 to the Victim's Wallet. ***Tx Hash 102***. Once again, at 12:59:47 PM, 0.0019605642794933 ETH was transferred from the Victim's Wallet to W2. ***Tx Hash 103.*** For the third time, at 1:06:23 PM, 0.003 ETH was transferred from W1 to the Victim's Wallet. ***Tx Hash 104***.

Finally, the first transaction, in the chart above, occurred at 1:07:35 PM where 0.0029866439308113 ETH was transferred from the Victim's Wallet to 0x829c23f7df91897f82edda60186abce9cbd191e6 ("W3"). ***Tx Hash 105***.

W.2 Transaction 2

The second transaction occurred at 1:08:59 PM where 0.0029012074536237 ETH was transferred from W3 to 0x53f001dfc267925993631398881efd5befeb9ac4 ("W4"). ***Tx Hash 106***. The funds are still there.

W.3 Transaction 3

At 1:08:59 PM, W1 infused money into the Victim's Wallet for the fourth time. At 1:08:59 PM, 0.003 ETH was transferred from W1 to the Victim's Wallet. ***Tx Hash 107***.

W.4 Transaction 4

The fourth transaction occurred at 1:09:47 PM where 0.0029496 ETH was transferred from the Victim's Wallet to W3. ***Tx Hash 108***.

W.5 Transaction 5

The fifth transaction occurred at 1:10:59 PM where 0.0029507564926086 ETH was transferred from the W3 to 0x792194dad565197d3cabdebb612f66f05fc346f0 ("W5"). ***Tx Hash 109***.

W.6 Transaction 6

As mentioned in Transaction W.1, two transactions were sent to W2 totaling .011914617 ETH. The sixth transaction occurred at 1:12:47 PM where 0.0118550595907542 ETH was transferred from W2 to V1, which is potentially a REMITANO account holder address. ***Tx Hash 110***.

W.7 Transaction 7

The seventh transaction occurred at 1:19:35 PM where 0.0117728397668862 ETH was transferred from V1 to V2, which is a REMITANO Hot Wallet. ***Tx Hash 111***.

W.8 Transaction 8

The eighth transaction occurred at 1:24:23 PM where 0.0028982564926086 ETH was transferred from W5 to the Victim's Wallet. ***Tx Hash 112***. In essence, this was a return of funds from Transaction W.5 minus Transaction Fees.

W.9 Transaction 9

The ninth transaction occurred at 1:25:23 PM where 0.0028020555407154 ETH was transferred from the Victim's Wallet to W2. ***Tx Hash 113***.

W.10 Transaction 10

For the fifth time on 8/22/2024, the Victim's Wallet appeared to need more Ethereum to cover Transaction Fees. The tenth transaction occurred at 2:18:23 PM where 0.00229781395670458 ETH was transferred from 0xc43ffdb7c154bf16d4862370969cdc1b77804027 ("W6") to the Victim's Wallet. ***Tx Hash 114***.

W.11 Transaction 11

The failed eleventh transaction occurred at 2:19:23 PM where there was an "Approve" Call Function to transact Mr. Gonzalez's KardiaChain Tokens which resulted in the following error message: "Warning! Error encountered during contract execution **[execution reverted]**." ***Tx Hash 115***.

W.12 Transaction 12

The twelfth transaction occurred at 2:19:59 PM where 0.00225210241547176 ETH was transferred from the Victim's Wallet to W5. ***Tx Hash 116***.

W.13 Transaction 13

The thirteenth transaction occurred at 2:27:47 PM where 0.0001 ETH was returned from W5 to the Victim's Wallet. ***Tx Hash 117***.

W.14 Transaction 14

There was yet another failed attempt to move Mr. Gonzalez's KardiaChain Tokens. The fourteenth transaction occurred at 2:28:23 PM where there was an "Transfer" Call Function to transact Mr. Gonzalez's KardiaChain Tokens which resulted in the following error message: "Warning! Error encountered during contract execution **[execution reverted]**; ERC-20 Token Transfer Error (Unable to locate corresponding Transfer Event Logs), Check with Sender." ***Tx Hash 118***.

W.15 Transaction 15

The fifteenth transaction occurred at 3:19:35 PM where 0.0027316475579514 ETH was returned from W2 to the Victim's Wallet. ***Tx Hash 119***. This appeared to be a reversal of transaction W.9.

W.16 Transaction 16

At 3:20:47 PM, an "Initiate Withdrawal" Function Call was conducted on Mr. Gonzalez's TrustSwap Tokens. ***Tx Hash 120***.

W.17 Transaction 17

The seventeenth transaction occurred at 3:24:23 PM where 0.00231567578513969 ETH was transferred from the Victim's Wallet to W2. ***Tx Hash 121***.

W.18 Transaction 18

There was yet another failed attempt to move Mr. Gonzalez's KardiaChain Tokens. The fourteenth transaction occurred at 10:26:59 PM where there was an "Transfer" Call Function to transact Mr. Gonzalez's Curve.fi: CRV Tokens which resulted in the following error message: "Warning! Error encountered during contract execution [out of gas]; ERC-20 Token Transfer Error (Unable to locate corresponding Transfer Event Logs), Check with Sender." ***Tx Hash 122***.

W.19 Transaction 19

The nineteenth transaction occurred on 8/29/2024 at 3:23:23 PM where 0.00218869718108669 ETH was returned from W2 to the Victim's Wallet. ***Tx Hash 123***. This appeared to be a reversal of Transaction W.17.

XII. TRACE X

X.1 Transaction 1 – **TrustSwap** Tokens and Ethereum stolen from the Victim Wallet

Date Time (GMT)	Hash	Receiving Wallet	Receiving Address	Amount	Token
8/29/24 3:39:11 PM	***Tx Hash 125***	W2	0x75b4cac515db8b4c154b77ff2 da0778c1441f766	426.101647	SWAP
8/29/24 3:39:59 PM	***Tx Hash 126***	W2	0x75b4cac515db8b4c154b77ff2 da0778c1441f766	0.000783083	ETH
8/30/24 8:38:35 AM	***Tx Hash 130***	W2	0x75b4cac515db8b4c154b77ff2 da0778c1441f766	0.003737219	ETH

On 8/29/2024 at 3:24:47 PM, there was a "Execute Withrawal" Call Function for Mr. Gonzalez's TrustSwap Tokens which resulted in two withdrawals of 401.227194275528 SWAP and 24.8744527401905 SWAP, respectively, to the Victim's Wallet. ***Tx Hash 124.*** At 3:39:11 PM, 426.101647015719 SWAP was transferred from the Victim's Wallet to W2. ***Tx Hash 125.***

X.2 Transaction 2

The second transaction occurred on 8/29/2024 at 3:39:59 PM where 0.000783083226274685 ETH was transferred from the Victim's Wallet to W2. ***Tx Hash 126***.

V.3 Transaction 3

The third transaction occurred on 8/30/2024 at 8:23:47 AM where 426.101647015719 STAKE was converted to 0.0186055982687701 ETH using MIMIC SWAPPER and returned to W2. ***Tx Hash 127***.

X.4 Transaction 4

The fourth transaction occurred on 8/30/2024 at 8:28:35 AM where 0.0174392726740583 ETH was transferred from W2 to V1, which is potentially a REMITANO account holder address. ***Tx Hash 128***.

X.5 Transaction 5

The fifth transaction occurred on 8/30/2024 at 8:38:59 AM where 0.0173722132486463 ETH was transferred from V1 to V2, which is a REMITANO Hot Wallet. ***Tx Hash 129***.

X.6 Transaction 6

The sixth transaction occurred on 8/30/2024 at 8:38:35 AM where 0.00373721884659906 ETH was transferred from the Victim's Wallet to W2. ***Tx Hash 130***.

X.6 Transaction 7

The seventh transaction occurred on 9/1/2024 at 12:08:35 AM where 0.00466235621035358 ETH was transferred from W2 to 0x4ab7849af9fabd73208a531c036c69b9d5ca4e43 ("X1") where the funds remain. ***Tx Hash 131***.

XII. OPPORTUNITY COSTS LOST DUE TO THEFT

5.1 CARE conducted an analysis of funds located in Mr. Gonzalez's wallet prior to the hack of his account on 5/8/2021. Of the 67 ERC-20 tokens and Ethereum, Mr. Gonzalez 26 of his ERC-20 Token assets stolen in addition to Ethereum. Since 5/8/2021, CARE discovered two additional assets that were transacted into Mr. Gonzalez's wallet that subsequently were removed. As explained below, the opportunity cost lost to Mr. Gonzalez due to the hack of his cryptocurrency wallet totaled $3,390,124,787,774.

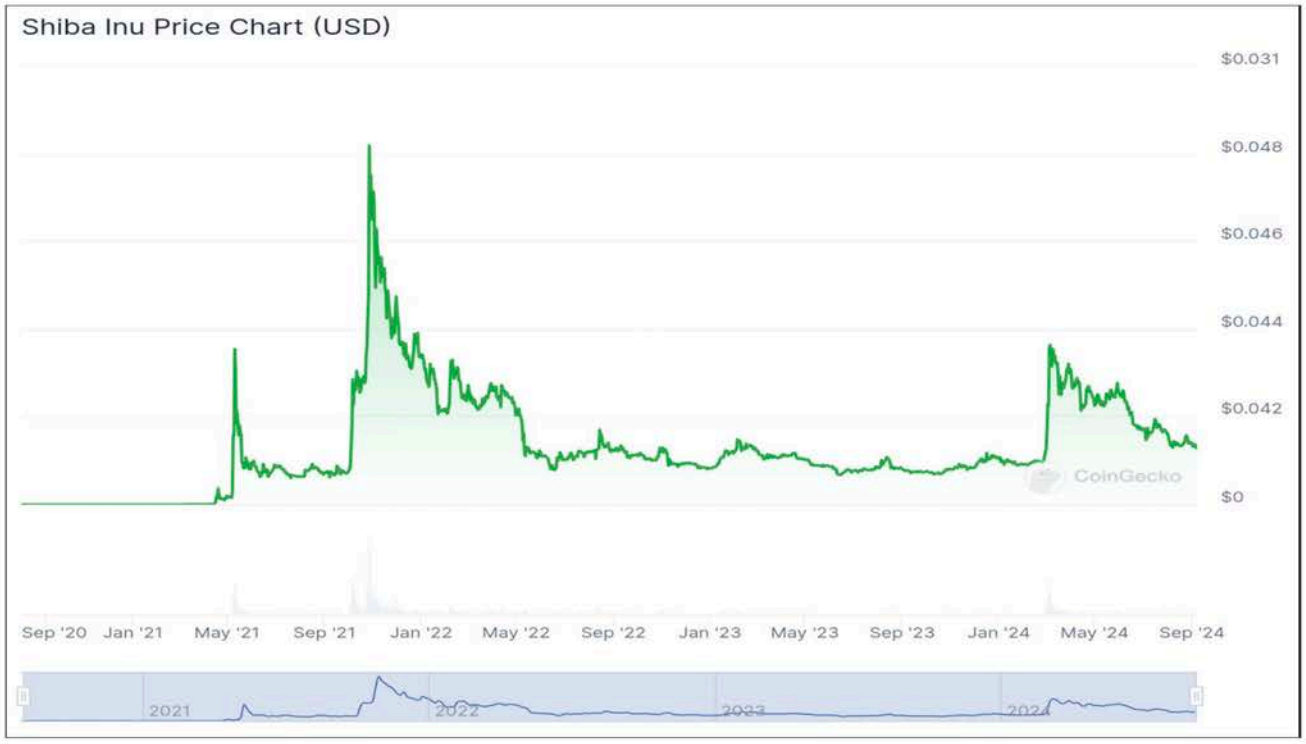
Token	Token Theft	Value of Theft	Max Price	Max Price Date	Lost Opp
SHIB	41,881,332,772.89	$657,205.10	0.00008616	10/28/2021	$3,608,496
HOKK	90,934,964,476,560.50	$113,728.81	0.03727	11/15/2021	$3,389,146,126,041
KISHU	6,677,846,866,673.65	$6,061.03	0.000000017550	5/15/2021	$117,196
AKITA	1,985,208,578.34	$9,909.60	0.00002904	5/11/2021	$57,650
FEG	1,382,788,310,243.34	$4,042.14	0.000705	12/29/2023	$974,865,759
HYDRO	53,436.64	$0.00	0.02477	8/30/2021	$1,324
PAID	123.3706939	$296.23	2.4	5/8/2021	$296
ETH	0.295111952	$1,154.70	4878.26	11/10/2021	$1,440
DGCL	578.2659609	$84.45	0.146040068	5/8/2021	$84
AAVE	0.55	$185.42	414.33	8/14/21	$229
AAVE	15.00	$5,600.33	414.33	8/14/21	$6,215
LID	2,618.25	$3.35	0.001305594	6/2/2021	$3
FTM	206.49	$72.22	3.46	10/28/2021	$714
SRM	14.06	$69.02	13.78	9/11/2021	$194
SXP	34.51	$75.00	3.8	8/26/2021	$131
MXC	3,790.22	$133.36	0.1335	1/19/2022	$506
AERGO	611.29	$117.19	0.425254	12/1/2021	$260
AKRO	3,127.37	$76.97	0.04277882	11/4/2021	$134
CVR	159.06	$47.22	0.296868292	6/2/2021	$47
RFuel	746.01	$30.63	0.094203	11/7/2021	$70
C3	140.00	$468.63	4.19	8/15/2021	$587

STAKE	2.10	$19.96	19.96	9/1/2021	$42
AXIAv3	40.32	$120.31	5.32	9/24/2021	$214
UBT	21.79	$72.92	3.346963799	9/19/2021	$73
YFBETA	1.19	$6.57	5.508995633	8/4/2024	$7
SWFL	81.06	$5.28	0.065135615	8/4/2024	$5
XAMP	1,832.24	$3.34	0.001822909	8/4/2024	$3
FRM	156.19	$3.37	0.021575915	8/4/2024	$3
SWAP	426.10	$45.21	0.116145	9/6/24	$49
					$3,390,124,787,774

5.2 Shiba Inu Tokens (SHIB)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
SHIB	41,881,332,772.89	5/8/21 1:13:51 PM	41,881,332,772.89	$657,205.10

On 9/6/2024, I conducted a search of coingecko.com for SHIB which revealed the following pricing chart[3]:



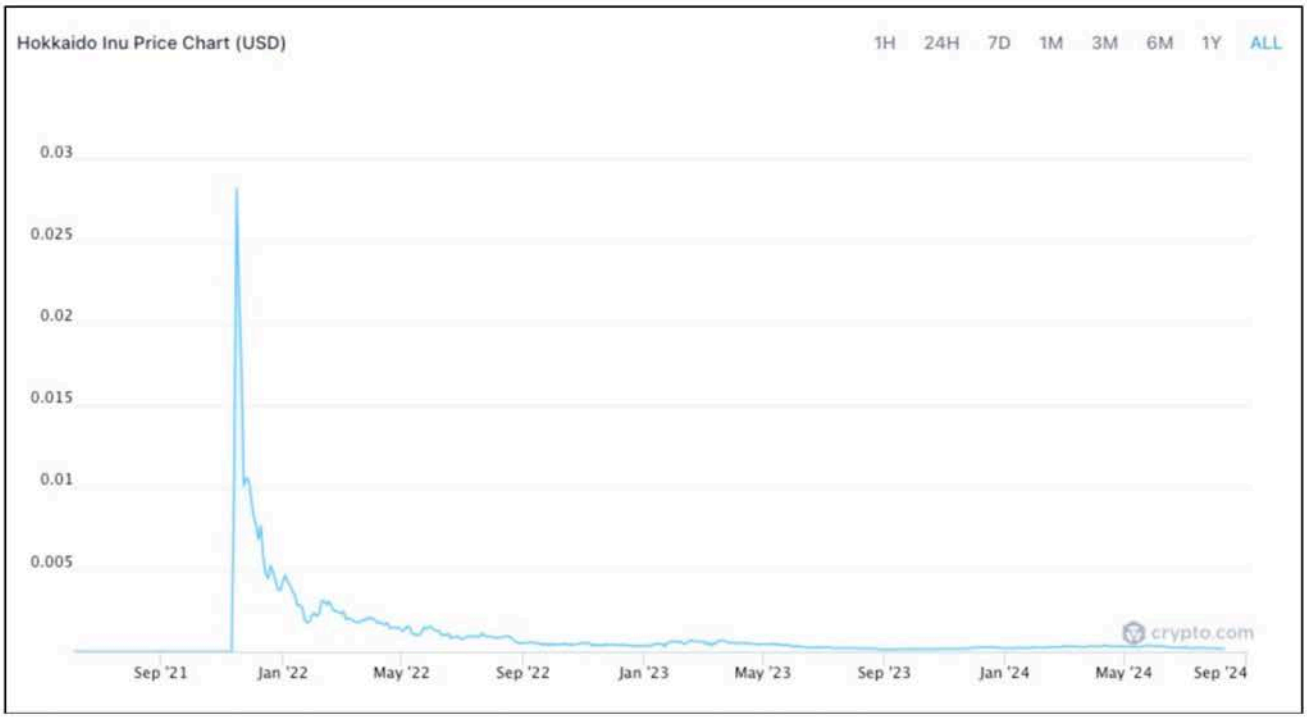
According to coingecko.com, SHIB realized its highest price of 0.00008616 on 10/28/2021. If Mr. Gonzalez's 41,881,332,772.89 SHIB was not stolen, he could have sold his SHIB on 10/28/2021 for **$3,608,495**.

[3] On 9/6/2024, I conducted a screen capture of coingecko.com for SHIB using Fireshot which is contained in Attachment 1.

5.3 Hokkaidu Inu Tokens (HOKK)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
HOKK	92,599,295,877,953.70	5/8/21 1:16:46 PM	90,934,964,476,560.50	$113,728.81

On 9/6/2024, I conducted a search of crypto.com for HOKK which revealed the following pricing chart[4]:



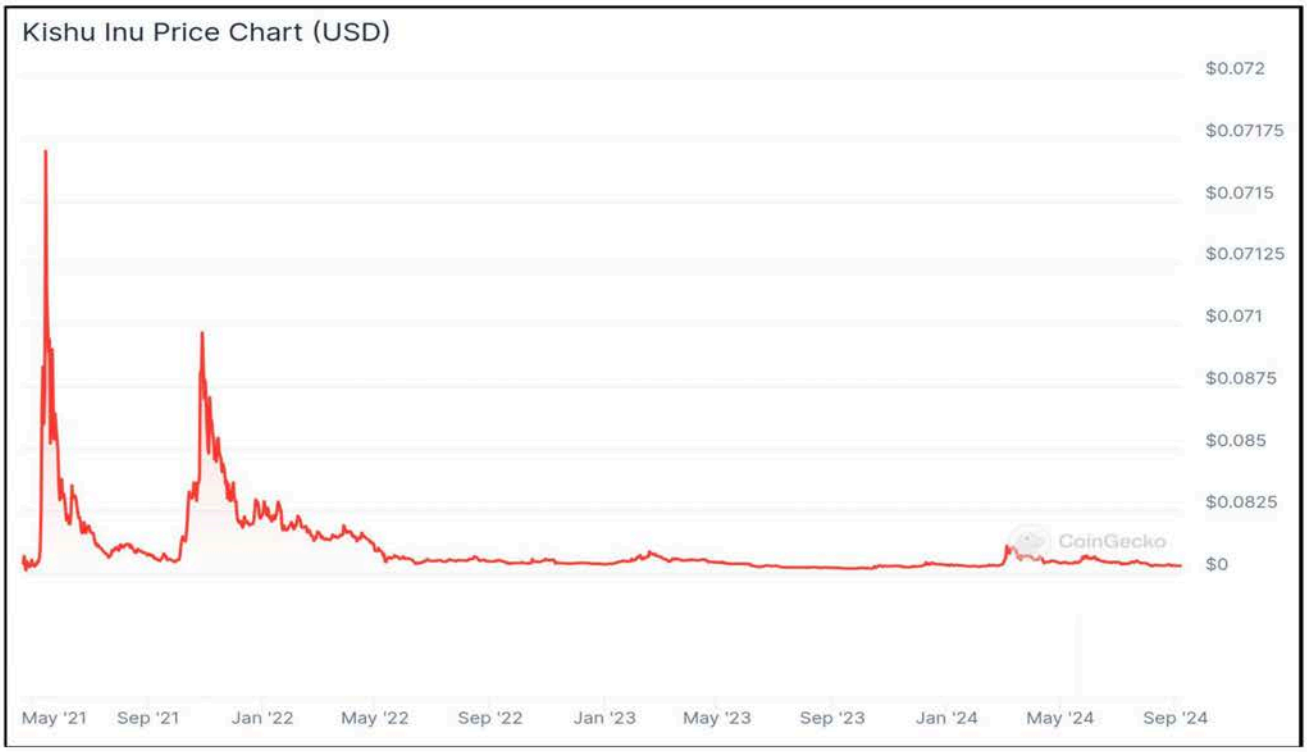
According to crypto.com, HOKK realized its highest price of 0.03727 on 11/15/2021. If Mr. Gonzalez's 41,881,332,772.89 HOKK was not stolen, he could have sold his HOKK on 11/15/2021 for **$3,389,146,126,041**. In fact, transaction hash 0x9b4ebcd9d2adb020abcfc03bb7fb95c54727fdbf87bb842f7846dd694a94bca1 occurred on 11/15/2021 where an individual sold 91,956,845,946 HOKK, far less HOKK in Mr. Gonzalez's possession when it was stolen, for $3,287,743,951. Even if Mr. Gonzalez missed the peak of HOKK's value by as much as a month, the price of HOKK was still as high as .004337 on 1/16/2022 which would have made Mr. Gonzalez's HOKK worth **$401,603,146,222**.

[4] On 9/6/2024, I conducted a screen capture of crypto.com for HOKK using Fireshot which is contained in Attachment 2.

5.4 Kishu Inu Tokens (KISHU)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
KISHU	6,789,990,932,636.93	5/8/21 1:16:46 PM	6,677,846,866,673.65	$6,061.03

On 9/6/2024, I conducted a search of coingecko.com for KISHU which revealed the following pricing chart[5]:



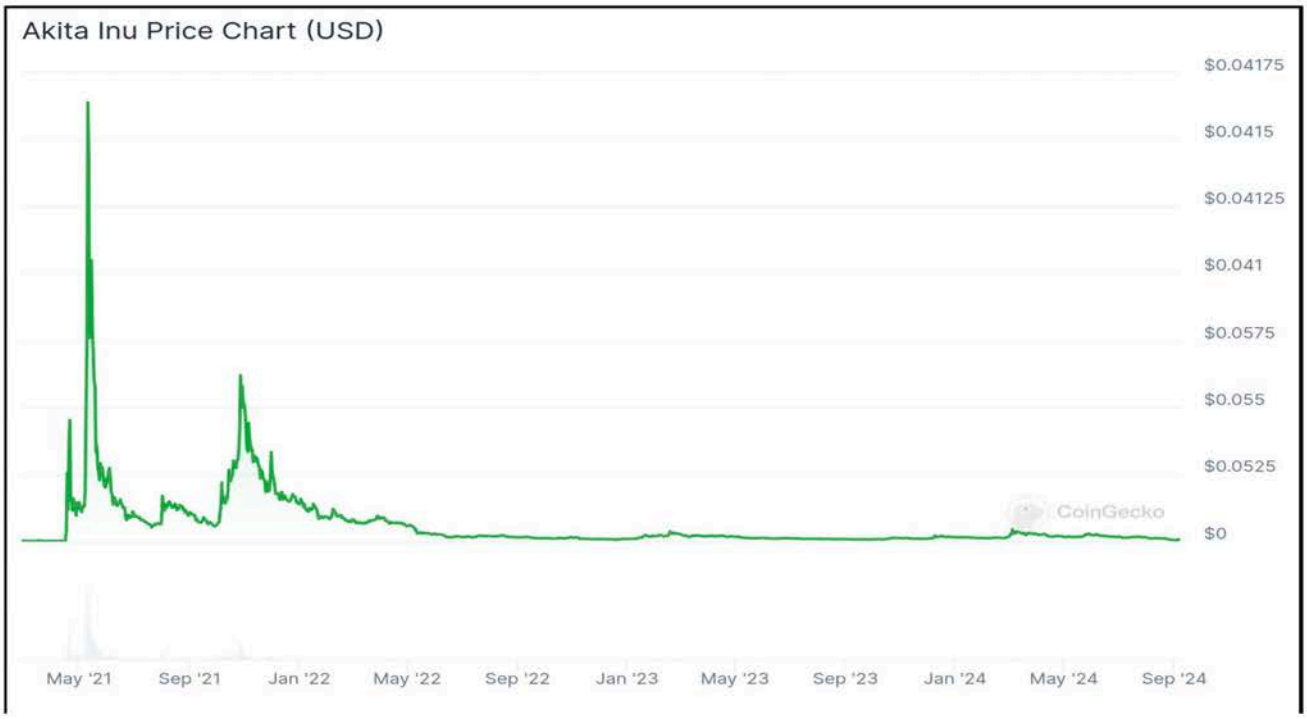
According to coingecko.com, KISHU realized its highest price of 0.00000001755 on 5/15/2021. If Mr. Gonzalez's 6,677,846,866,673.65 KISHU was not stolen, he could have sold his KISHU on 5/15/2021 for **$117,196**.

[5] On 9/6/2024, I conducted a screen capture of coingecko.com for KISHU using Fireshot which is contained in Attachment 3.

5.5 Akita Inu Tokens (AKITA)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
AKITA	1,985,208,578.34	5/8/21 1:16:46 PM	1,985,208,578.34	$9,909.60

On 9/6/2024, I conducted a search of coingecko.com for AKITA which revealed the following pricing chart[6]:



According to coingecko.com, AKITA realized its highest price of 0.00002904 on 5/11/2021. If Mr. Gonzalez's 1,985,208,578.34349 AKITA was not stolen, he could have sold his AKITA on 5/11/2021 for **$57,650**.

[6] On 9/6/2024, I conducted a screen capture of coingecko.com for AKITA using Fireshot which is contained in Attachment 4.

5.6 FEG Tokens (FEG), aka "Old FEG Token"

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
FEG	1,410,792,754,419.82	5/8/21 1:16:46 PM	1,382,788,310,243.34	$4,042.14

On 9/6/2024, I conducted a search of coincarp.com for FEG which revealed the following pricing chart[7]:

According to coincarp.com, FEG realized its highest price of 0.000705 on 12/29/2023. If Mr. Gonzalez's 11,382,788,310,243.34 FEG was not stolen, he could have sold his FEG on 12/29/2023 for **$974,865,758**. From 9/25/2023 to 1/29/2024, FEG experienced a spike in price. On 9/25/2023, the price rose to .000236, hit its peak on 12/29/2023, and didn't drop significantly until just after 1/29/2024 when it was still as a high as .000625. The lowest price in that four month time period occurred on 11/2/2023 where it dipped to .000107. Even during that dip on 11/2/2023, Mr. Gonzalez's FEG would have been worth **$147,958,349**.

[7] On 9/6/2024, I conducted a screen capture of livecoinwatch.com for FEG using Fireshot which is contained in Attachment 5.

5.7 Hydro Tokens (HYDRO)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
HYDRO	53,436.64	5/8/21 1:16:46 PM	53,436.64	$0.00

On 9/6/2024, I conducted a search of crypto.com for HYDRO which revealed the following pricing chart[8]:

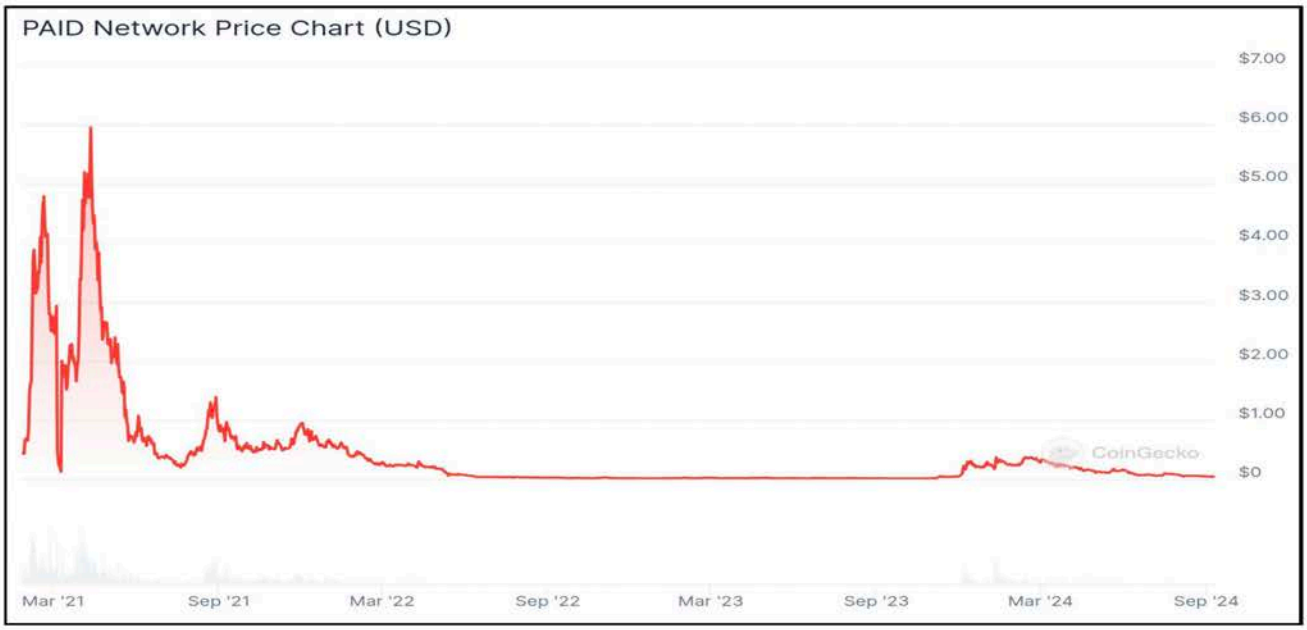
According to crypto.com, HYDRO realized its highest price of 0.02477 on 8/30/2021. If Mr. Gonzalez's 53436.6429452757 HYDRO was not stolen, he could have sold his HYDRO on 8/30/2021 for **$1,323**.

[8] On 9/9/2024, I conducted a screen capture of crypto.com for HYDRO using Fireshot which is contained in Attachment 6.

5.8 PAID Network Tokens (PAID)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
HYDRO	53,436.64	5/8/21 1:16:46 PM	53,436.64	$0.00

On 9/9/2024, I conducted a search of coingecko.com for PAID which revealed the following pricing chart[9]:



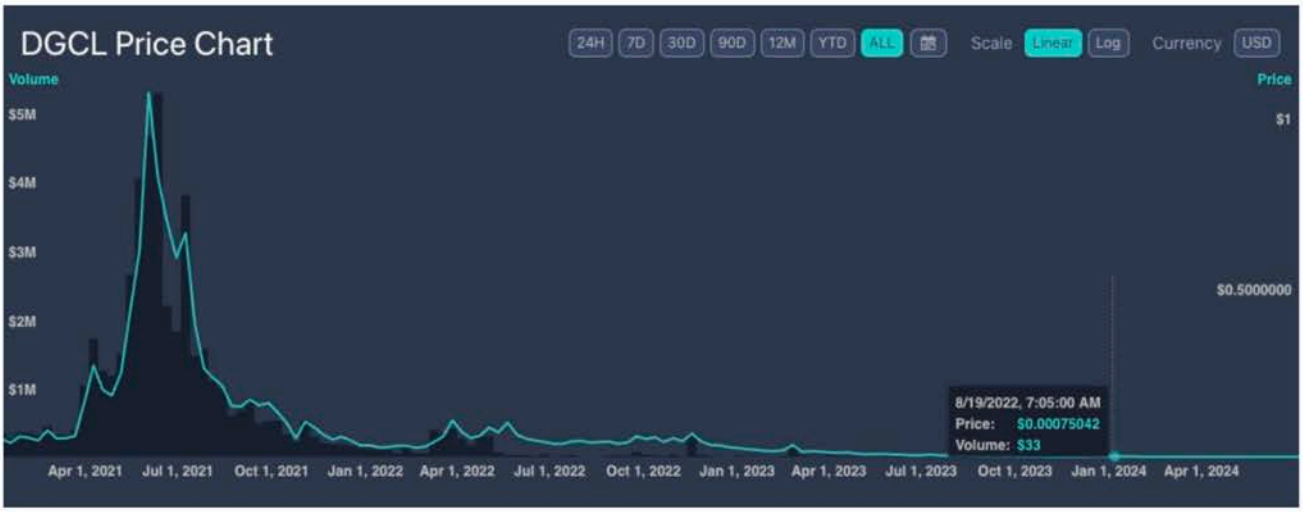
According to coingecko.com, PAID had a declining value after it was stolen so its highest value occurred on 5/8/2021.

[9] On 9/9/2024, I conducted a screen capture of coingecko.com for PAID using Fireshot which is contained in Attachment 7.

5.9 DigiCol Tokens (DGCL)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
DGCL	578.2659609	5/8/21 3:53:20 PM	578.2659609	$84.45

On 9/9/2024, I conducted a search of livecoinwatch.com for DGCL which revealed the following pricing chart[10]:



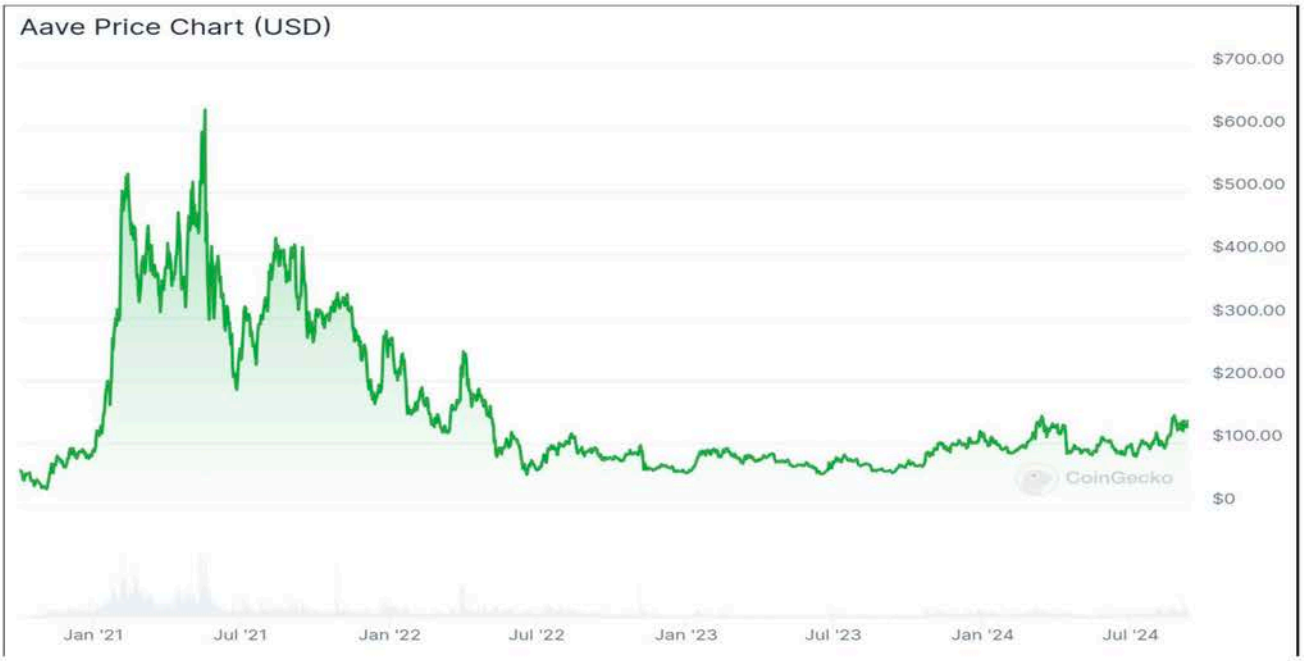
According to livecoinwatch.com, DGCL had a declining value after it was stolen so its highest value occurred on 5/8/2021.

[10] On 9/9/2024, I conducted a screen capture of livecoinwatch.com for DGCL using Fireshot which is contained in Attachment 8.

5.10 Staked Aave Tokens (stkAAVE)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
stkAAVE	15	6/1/21 12:19:41 PM	15.00	$5,600.33

On 9/9/2024, I conducted a search of coingecko.com for stkAAVE which revealed the following pricing chart[11]:



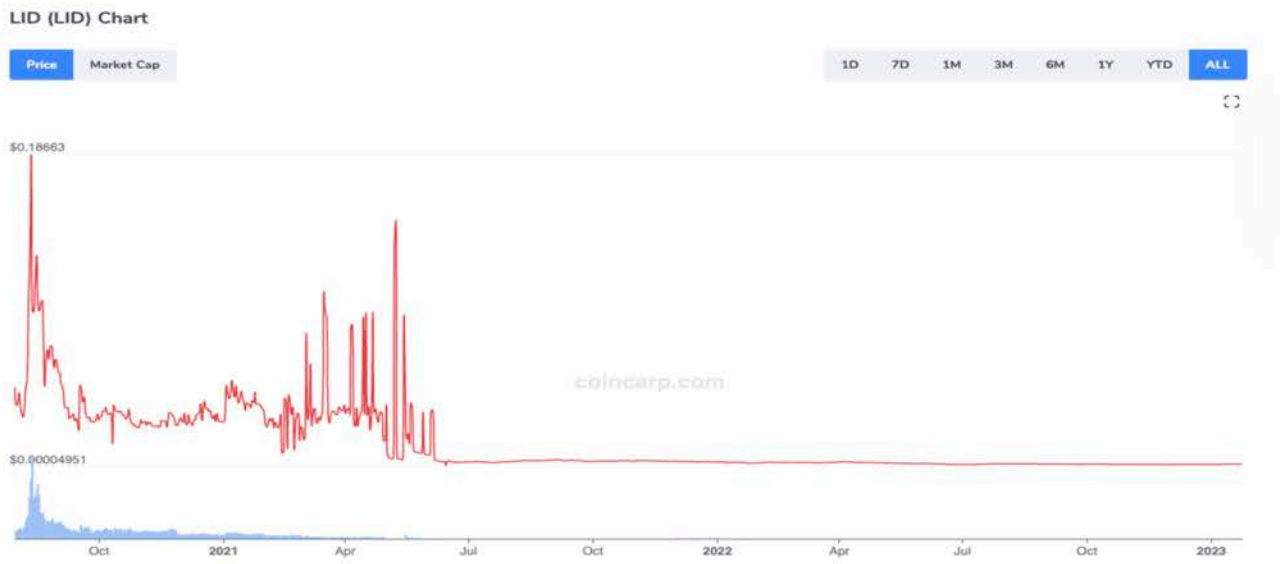
According to coingecko.com, stkAAVE realized its highest price of 414.33 on 8/14/2021. If Mr. Gonzalez's 414.33 stkAAVE was not stolen, he could have sold his stkAAVE on 8/14/2021 for **$6,214**.

[11] On 9/9/2024, I conducted a screen capture of coingecko.com for stkAAVE using Fireshot which is contained in Attachment 9.

5.11 Liquidity Dividends Protocol Tokens (LID)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
LID	2,618.25	6/2/21 10:58:00 AM	2,618.25	$3.35

On 9/9/2024, I conducted a search of coincarp.com for LID which revealed the following pricing chart[12]:



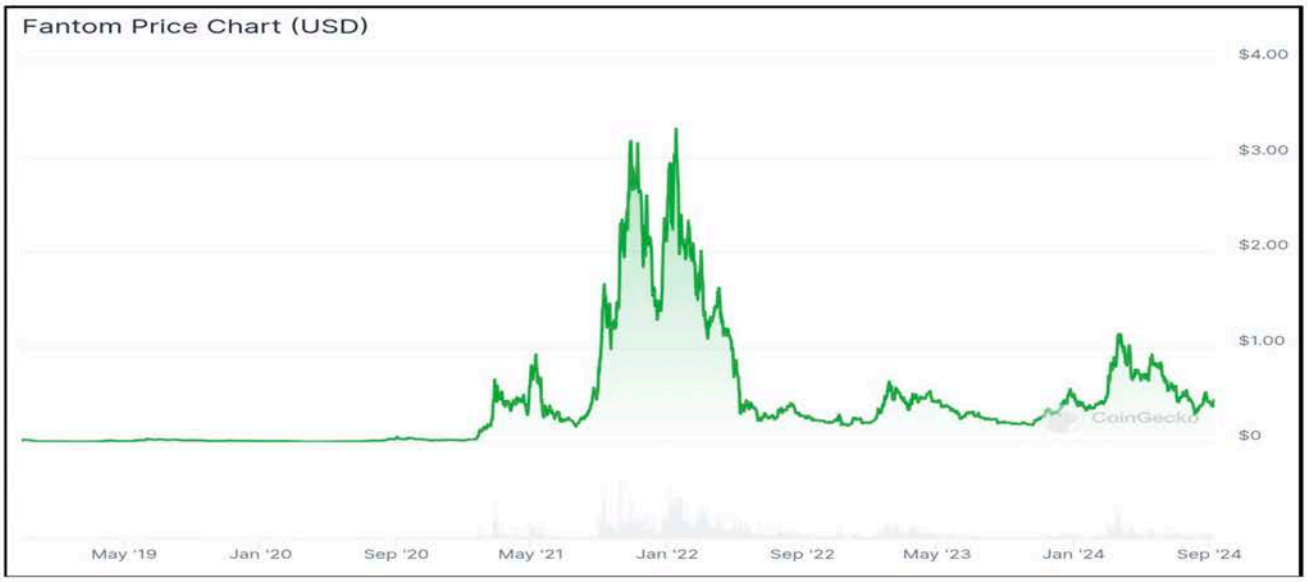
According to coincarp.com, LID had a declining value after it was stolen so its highest value occurred on 6/2/2021.

[12] On 9/9/2024, I conducted a screen capture of coincarp.com for LID using Fireshot which is contained in Attachment 10.

5.12 Fantom Tokens (FTM)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
FTM	206.4917824	6/2/21 10:58:48 AM	206.49	$72.22

On 9/9/2024, I conducted a search of coingecko.com for FTM which revealed the following pricing chart[13]:



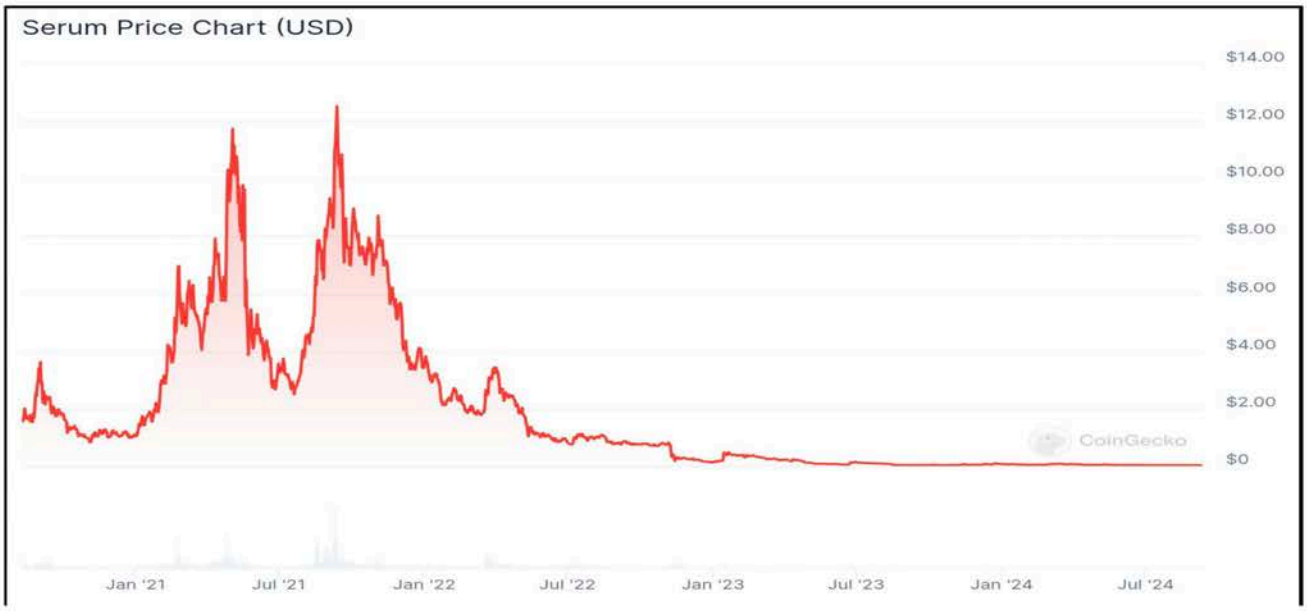
According to coingecko.com, FTM realized its highest price of 3.46 on 10/28/2021. If Mr. Gonzalez's 206.49178244133 FTM was not stolen, he could have sold his FTM on 10/28/2021 for **$714**.

[13] On 9/9/2024, I conducted a screen capture of coingecko.com for FTM using Fireshot which is contained in Attachment 11.

5.13 Serum Tokens (SRM)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
SRM	14.058493	6/2/21 11:02:06 AM	14.06	$69.02

On 9/9/2024, I conducted a search of coingecko.com for SRM which revealed the following pricing chart[14]:



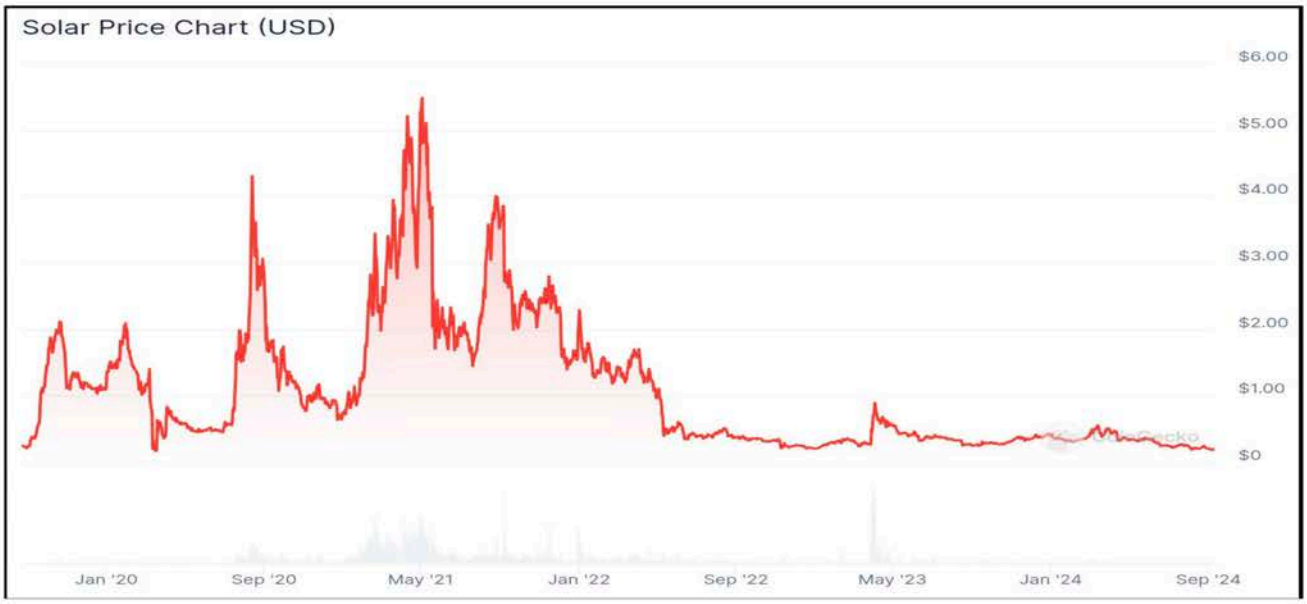
According to coingecko.com, SRM realized its highest price of 13.78 on 9/11/2021. If Mr. Gonzalez's 14.058493 SRM was not stolen, he could have sold his SRM on 9/11/2021 for **$193**.

[14] On 9/9/2024, I conducted a screen capture of coingecko.com for SRM using Fireshot which is contained in Attachment 12.

5.14 Swipe Tokens (SXP)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
SXP	34.5149981	6/2/21 11:02:18 AM	34.51	$75.00

On 9/9/2024, I conducted a search of coingecko.com for SXP which revealed the following pricing chart[15]:



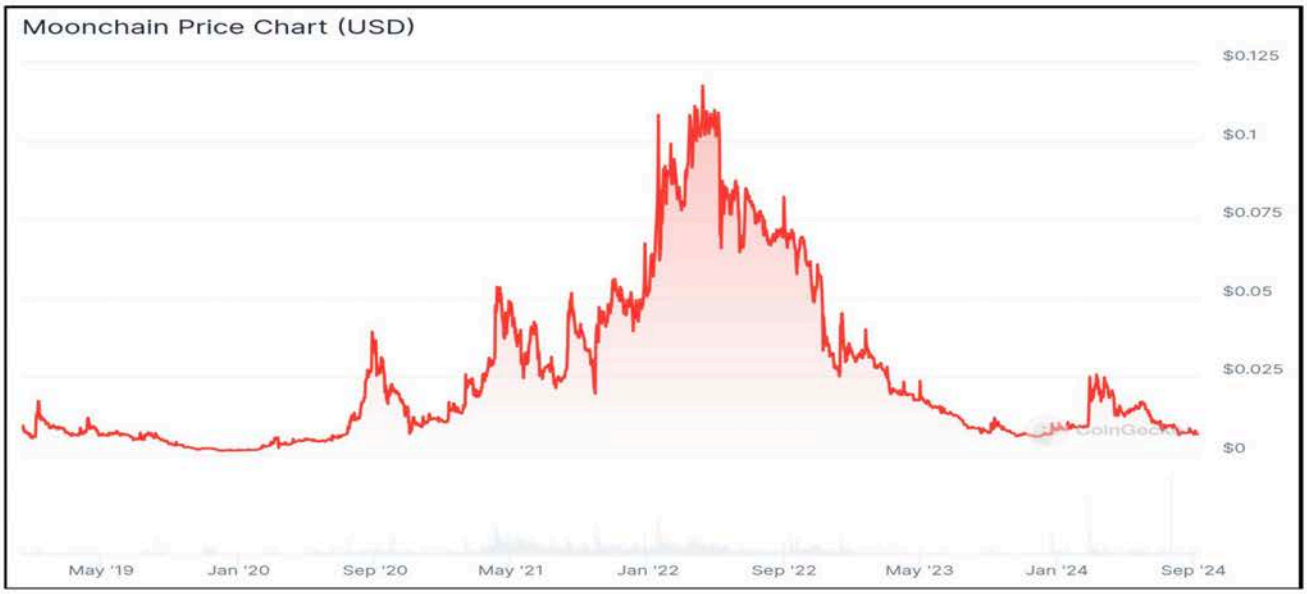
According to coingecko.com, SXP realized its highest price of 3.8 on 8/26/2021. If Mr. Gonzalez's 34.514998102642 SXP was not stolen, he could have sold his SXP on 8/26/2021 for **$131**.

[15] On 9/9/2024, I conducted a screen capture of coingecko.com for SXP using Fireshot which is contained in Attachment 13.

5.15 MXC Tokens (MXC)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
MXC	3,790.22	6/2/21 11:11:44 AM	3,790.22	MXC

On 9/9/2024, I conducted a search of coingecko.com for MXC which revealed the following pricing chart[16]:



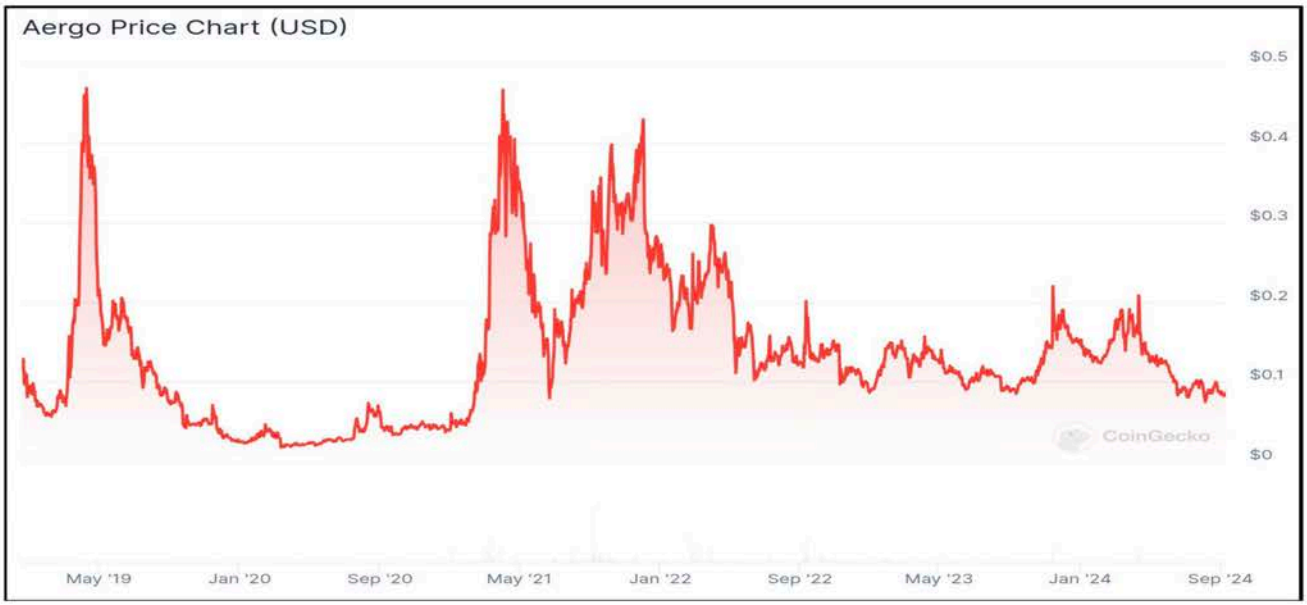
According to coingecko.com, MXC realized its highest price of 0.1335 on 1/19/2022. If Mr. Gonzalez's 3,790.21814260124 MXC was not stolen, he could have sold his MXC on 1/19/2022 for **$506**.

[16] On 9/9/2024, I conducted a screen capture of coingecko.com for MXC using Fireshot which is contained in Attachment 14.

5.16 Aergo Tokens (AERGO)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
AERGO	611.2925109	6/2/21 11:11:44 AM	611.29	$117.19

On 9/9/2024, I conducted a search of coingecko.com for AERGO which revealed the following pricing chart[17]:



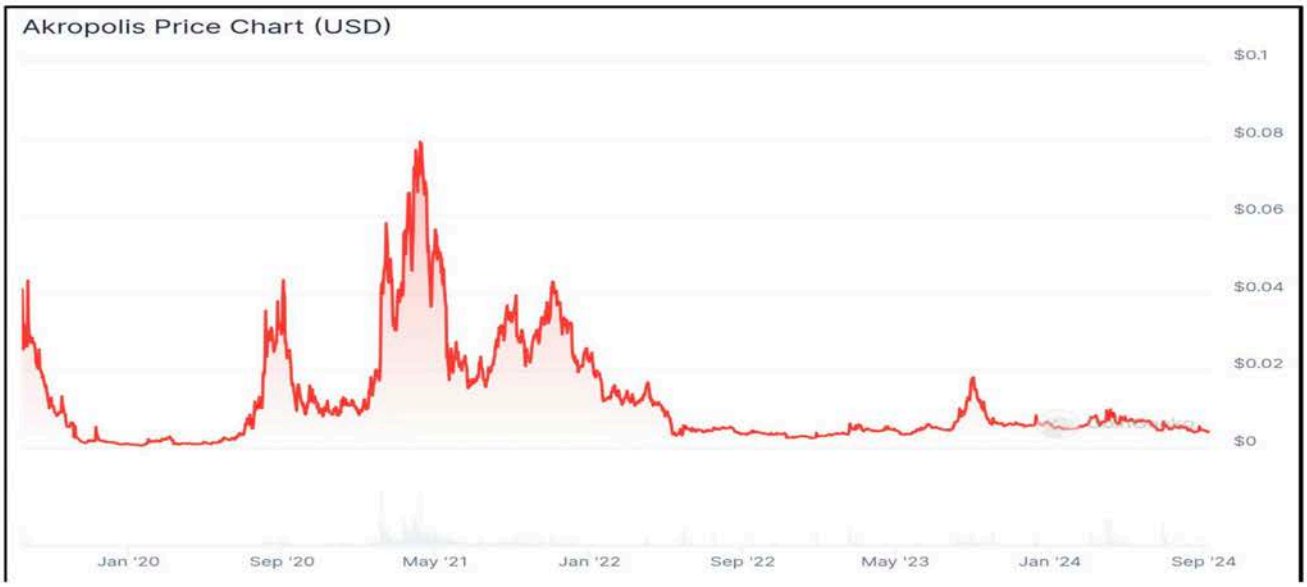
According to coingecko.com, AERGO realized its highest price of 0.425254 on 12/1/2021. If Mr. Gonzalez's 611.29251086567 AERGO was not stolen, he could have sold his AERGO on 12/1/2021 for **$260**.

[17] On 9/9/2024, I conducted a screen capture of coingecko.com for AERGO using Fireshot which is contained in Attachment 15.

5.17 Akropolis Tokens (AKRO)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
AKRO	3,127.37	6/2/21 11:12:50 AM	3,127.37	$76.97

On 9/9/2024, I conducted a search of coingecko.com for AKRO which revealed the following pricing chart[18]:



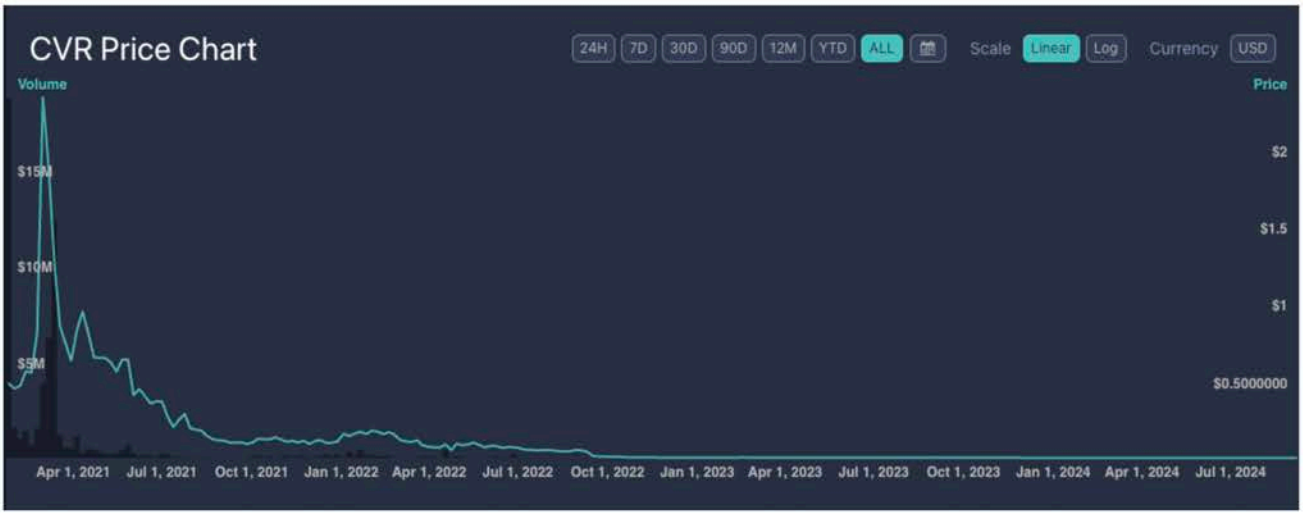
According to coingecko.com, AKRO realized its highest price of 0.04277882 on 11/4/2021. If Mr. Gonzalez's 3127.36791500478 AKRO was not stolen, he could have sold his AKRO on 11/4/2021 for **$134**.

[18] On 9/9/2024, I conducted a screen capture of coingecko.com for AKRO using Fireshot which is contained in Attachment 16.

5.18 PolkaCover Tokens (CVR)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
CVR	159.0604363	6/2/21 11:24:19 AM	159.06	CVR

On 9/9/2024, I conducted a search of livecoinwatch.com for CVR which revealed the following pricing chart[19]:



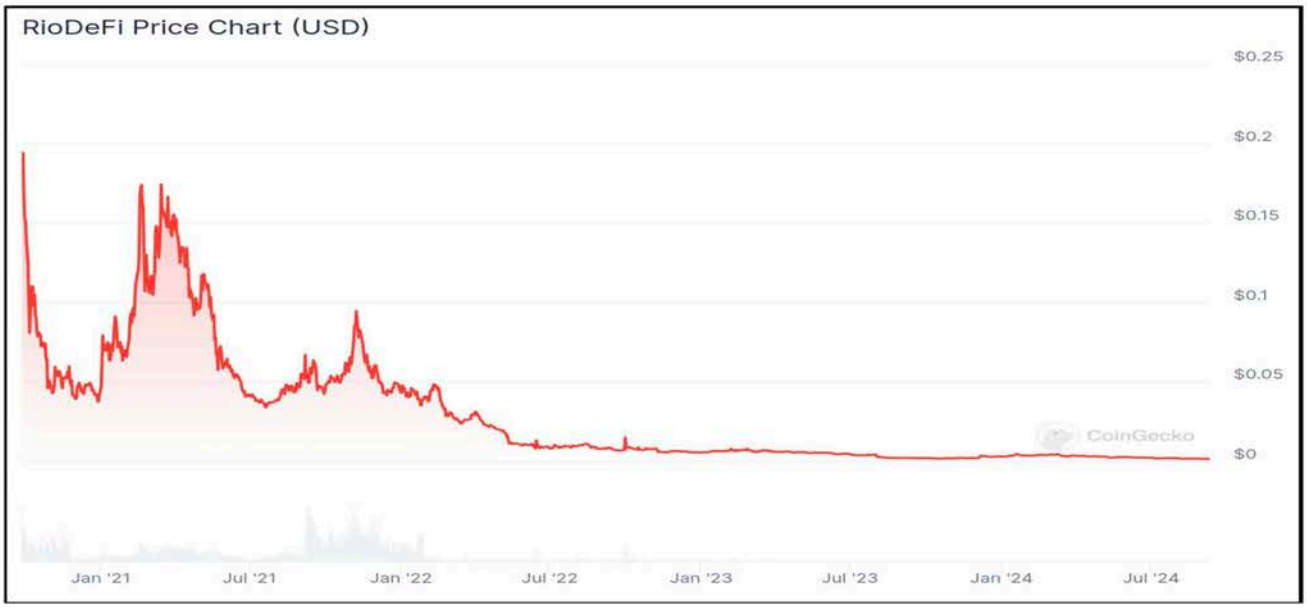
According to livecoinwatch.com, CVR had a declining value after it was stolen so its highest value occurred on 6/2/2021.

[19] On 9/9/2024, I conducted a screen capture of livecoinwatch.com for CVR using Fireshot which is contained in Attachment 17.

5.19 Rio Fuel Tokens (RFuel)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
RFuel	746.0104865	7/1/21 3:13:28 PM	746.01	RFuel

On 9/9/2024, I conducted a search of coingecko.com for RFuel which revealed the following pricing chart[20]:



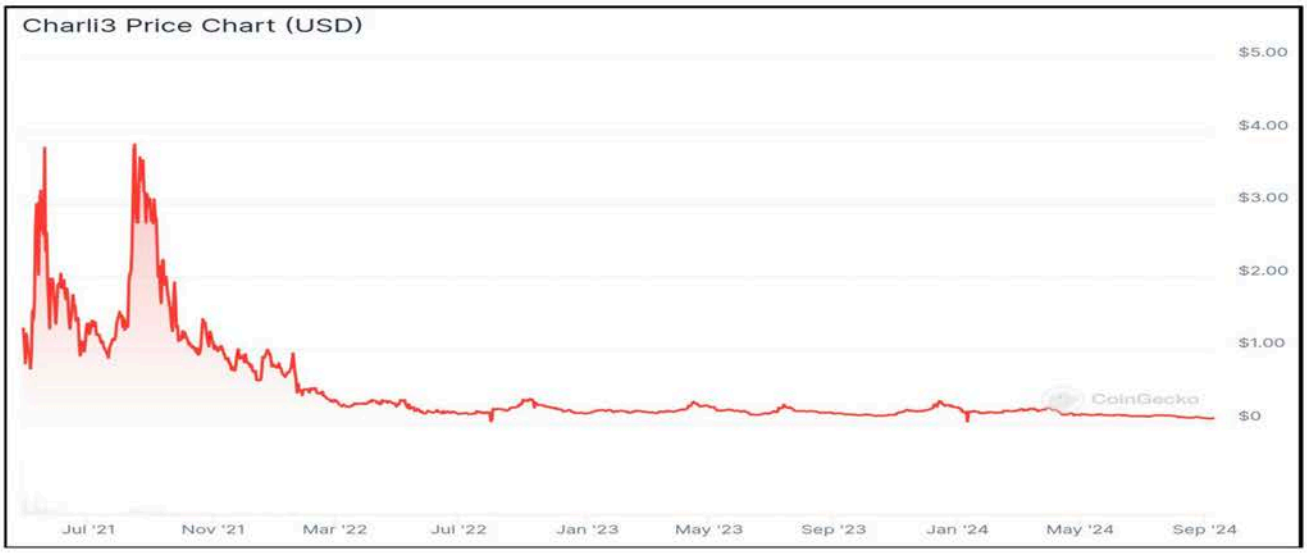
According to coingecko.com, RFuel realized its highest price of 0.094203 on 11/7/2021. If Mr. Gonzalez's 746.010486472624 RFuel was not stolen, he could have sold his RFuel on 11/7/2021 for **$70**.

[20] On 9/9/2024, I conducted a screen capture of coingecko.com for RFuel using Fireshot which is contained in Attachment 18.

5.20 Charli3 Tokens (C3)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
C3	139.9968407	8/21/21 6:51:17 AM	140.00	$468.63

On 9/9/2024, I conducted a search of coingecko.com for C3 which revealed the following pricing chart[21]:



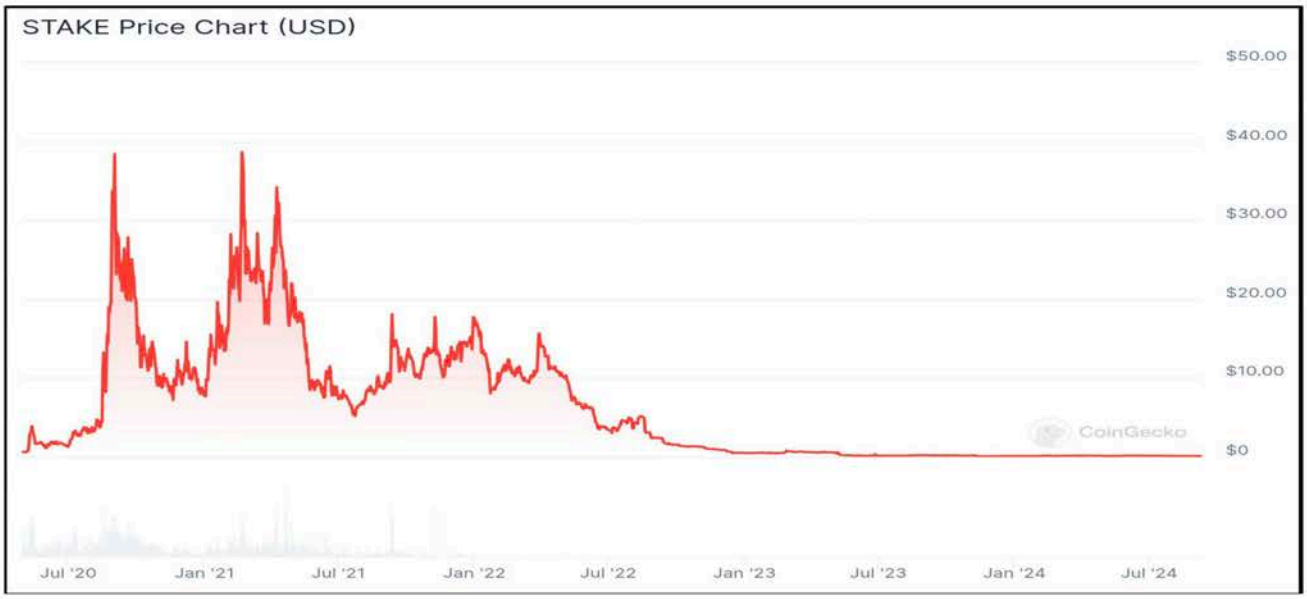
According to coingecko.com, C3 realized its highest price of 4.19 on 8/15/2021. If Mr. Gonzalez's 139.996840673394 C3 was not stolen, he could have sold his C3 on 8/15/2021 for **$586**.

[21] On 9/9/2024, I conducted a screen capture of coingecko.com for C3 using Fireshot which is contained in Attachment 19.

5.21 Stake Tokens (STAKE)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
STAKE	2.097088785	9/1/21 4:21:51 AM	2.10	$19.96

On 9/9/2024, I conducted a search of coingecko.com for STAKE which revealed the following pricing chart[22]:



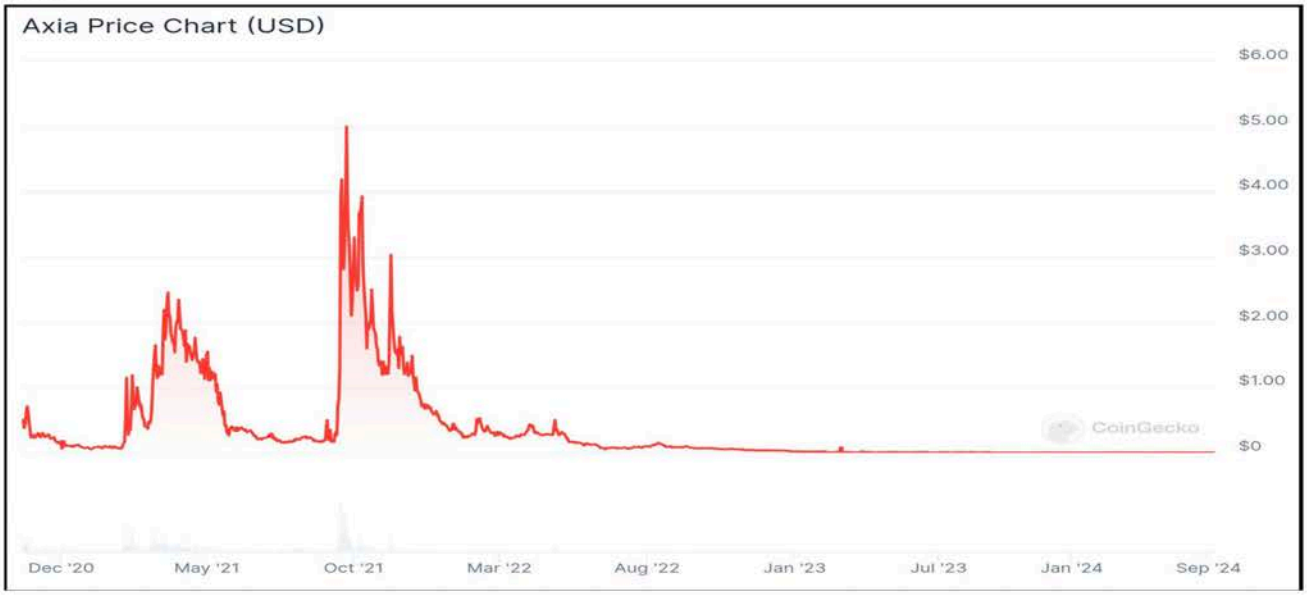
According to coingecko.com, STAKE had a declining value after it was stolen so its highest value occurred on 9/1/2021.

[22] On 9/9/2024, I conducted a screen capture of coingecko.com for STAKE using Fireshot which is contained in Attachment 20.

5.22 Axia Tokens (AXIAv3)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
AXIAv3	40.31788903	9/19/21 11:25:26 AM	40.32	AXIAv3

On 9/9/2024, I conducted a search of coingecko.com for AXIAv3 which revealed the following pricing chart[23]:



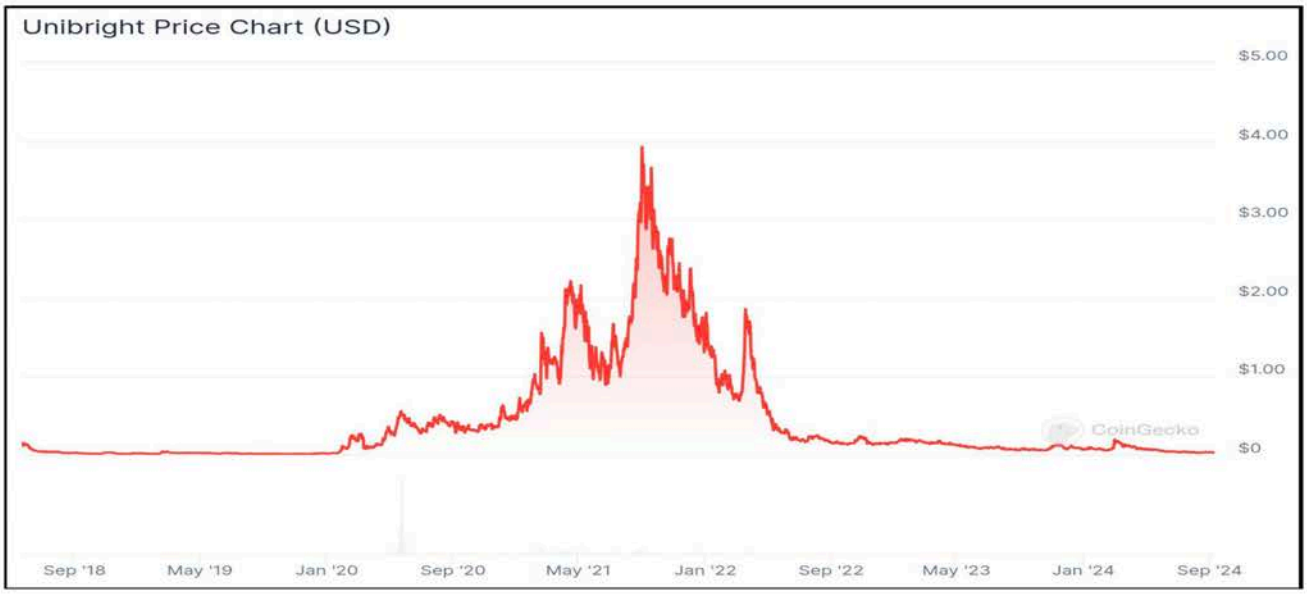
According to coingecko.com, AXIAv3 realized its highest price of 5.32 on 9/24/2021. If Mr. Gonzalez's 40.317889027807 AXIAv3 was not stolen, he could have sold his AXIAv3 on 9/24/2021 for **$214**.

[23] On 9/9/2024, I conducted a screen capture of coingecko.com for AXIAv3 using Fireshot which is contained in Attachment 21.

5.23 UniBright Tokens (UBT)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
UBT	21.78691028	9/19/21 11:29:03 AM	21.79	UBT

On 9/9/2024, I conducted a search of coingecko.com for UBT which revealed the following pricing chart[24]:



According to coingecko.com, UBT had a declining value after it was stolen so its highest value occurred on 9/19/2021.

[24] On 9/9/2024, I conducted a screen capture of coingecko.com for UBT using Fireshot which is contained in Attachment 22.

5.24 yfBETA Tokens (YFBETA)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
YFBETA	1.192594883	8/4/24 12:12:47 AM	1.19	YFBETA

On 9/9/2024, I conducted a search of coincarp.com for YFBETA which revealed the following pricing chart[25]:

According to coincarp.com, YFBETA had a declining value after it was stolen so its highest value occurred on 8/4/2024.

[25] On 9/9/2024, I conducted a screen capture of coincarp.com for YFBETA using Fireshot which is contained in Attachment 23.

5.25 Swapfolio Tokens (SWFL)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
SWFL	81.06164319	8/4/24 12:13:59 AM	81.06	SWFL

On 9/9/2024, I conducted a search of livecoinwatch.com for SWFL which revealed the following pricing chart[26]:

According to livecoinwatch.com, SWFL had a declining value after it was stolen so its highest value occurred on 8/4/2024.

[26] On 9/9/2024, I conducted a screen capture of livecoinwatch.com for SWFL using Fireshot which is contained in Attachment 24.

5.26 Antiample Tokens (XAMP)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
XAMP	1,888.32	8/4/24 12:15:23 AM	1,832.24	XAMP

On 9/9/2024, I conducted a search of livecoinwatch.com for XAMP which revealed the following pricing chart[27]:

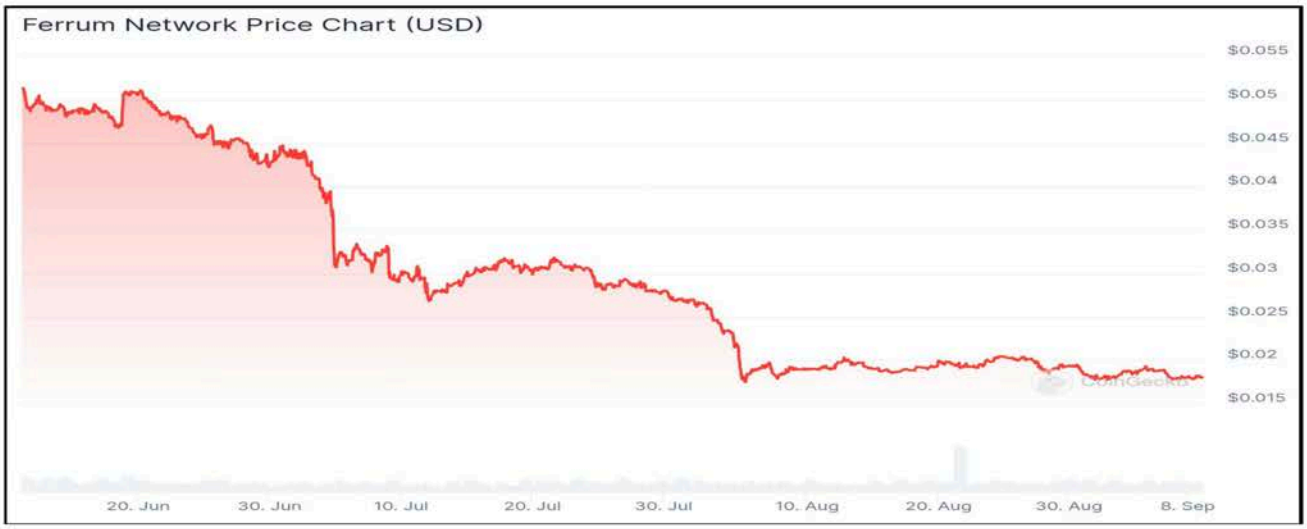
According to livecoinwatch.com, XAMP had a declining value after it was stolen so its highest value occurred on 8/4/2024.

[27] On 9/9/2024, I conducted a screen capture of livecoinwatch.com for XAMP using Fireshot which is contained in Attachment 25.

5.27 Ferrum Network Tokens (FRM)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
FRM	156.192684	8/4/24 12:16:59 AM	156.19	$3.37

On 9/9/2024, I conducted a search of coingecko.com for FRM which revealed the following pricing chart[28]:



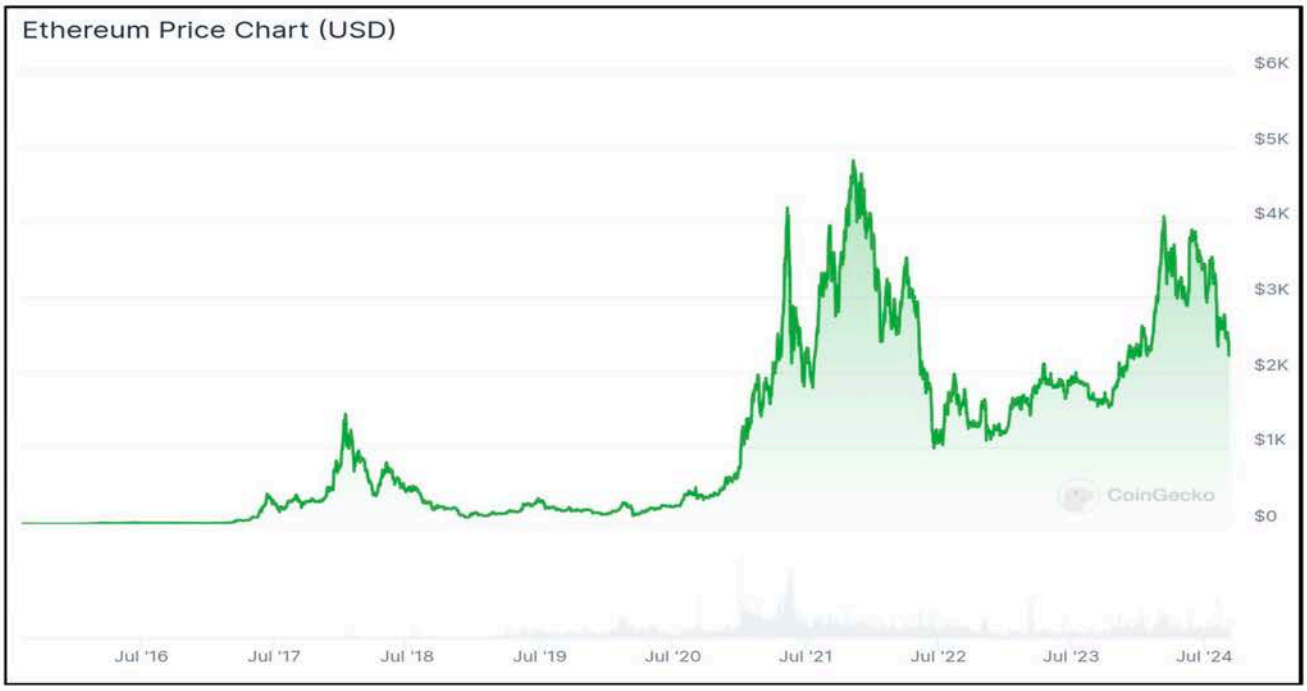
According to coingecko.com, FRM had a declining value after it was stolen so its highest value occurred on 8/4/2024.

[28] On 9/9/2024, I conducted a screen capture of coingecko.com for FRM using Fireshot which is contained in Attachment 26.

5.28 Ethereum (ETH)

Token	5/7/2021	Date of Theft	Token Theft	USD Value of Theft
ETH	0.295111952	5/8/21 1:25:23 PM	0.295111952	ETH

On 9/9/2024, I conducted a search of coingecko.com for ETH which revealed the following pricing chart[29]:



According to coingecko.com, ETH realized its highest price of 4,878.26 on 11/10/2021. If Mr. Gonzalez's 0.295111951726702 ETH was not stolen, he could have sold his ETH on 11/10/2021 for **$1,439**.

[29] On 9/9/2024, I conducted a screen capture of coingecko.com for ETH using Fireshot which is contained in Attachment 27.

XIII. HASH VALUES

Hash Label	Transaction Hash
33	0xf9030c4aba217a9c8e1103180a1fd42268e6df1566e97d6f92042965ed5d201d
34	0x1c21448a2fc5140ab379f60e29fd0efa54b3d6f50044fb46da2ee296a4395ba0
35	0x570e6656cec8b9390876374feed97af84a5da67609d707b2a5b2cf8a59e12c33
36	0x3e714c21341ab40b41aeba98a12f22b54a0ecdef5dc5ad356c7a2b3081337a93
37	0xd84101cbb56c8f6fa96af294fa9b85bc3c47e07ff1abdfd858a5eeaa0c24df70
38	0xb367e450bf1c0ffdad7e12d222900d8b686698c27a0646900fb3c7b3930eec00
39	0x64fe3c60539d41cd73bfafe1fb3fe376dc729193d27d1049b80c0679b07ca9d4
40	0x351f7edba3b0c9dc132809633ac7c61f9a01463c7187d2302da95953a7b70d61
41	0xd2e751bd22afa8188d1e03a1f953c6c41e41b04a248eb121b8c32bd5f128e2d2
42	0xff73b6b75ebc93e5cd6479d3149ee53a4ec352dba3cb9a83a5bb256c0948ea7c
43	0x713be83f94ed68895ebc4fb142ccdd2ff2b2ab58af0ac58a26624127e440807c
44	0xfa6a7fbfdb2bced10da882ae12073b6882e125caf48b024eb64158226a3415aa
45	0x049f109f84a7f0815d7192855b4be4c52622efd7acb34fc8dcb48378edfd425d
46	0xe18efd3636d9bda9728e4040da60de6a5f141bcad2a28b6ed294ab2d66f0a4b8
47	0x2f6946847d308f0038ff6a8b0982b6524312835975efb43a4a690c4bd024607d
48	0xffa62abd6e484a2704680c4007ea6d9ef9450934fa7b40a17647eeff955cb3e6
49	0x4e13291abc525f73aaad5a62f3446a5152830cfdf3a1ff96164a7c3caa701c11
50	0xe9615be7fff2e37fc55c60d99a0f5fd003cee455c5cb712e28ffbcbecc0ac557
51	0x7f03f381a18974b3598216650da499909e68a96d5ed6ebdebe4e55c3d777105c
52	0x68fdee2345b38680aae437379846aa6aca277db7e8a5df2a84207b2f005c3205
53	0xa693b2f4620a923762f772a3aaf5c4cbd36f10daf3a6b783b2ce9cf77f8f0bf8
54	0x4e98ef3f2022ecc4d79ff54f5baa4b1567b53ed275a09ce3eee693d1f54e4a8e
55	0xa9feeb38d97a64f983f610c42d4254e50b01244738256a9ae6e6d381ee8639d9
56	0xe636a3efcf189c56467476d04585e0cb5825d0788183d9efe59979e18068ac66
57	0x7e9a775f0a082d4945d2796f26da01a46633c1aa8498bfcbd441e08317d706c3
58	0x5dbc885790c63b7534da8efdb67162e778c48b0e43322bfd7817d47662f154cb
59	0xc99c5f1eb8f17bfab9d0799b0f3468670a9518aa58add447009c824202633b49
60	0xe30ac38f35287371e180752e024200273765b8b9bc89f9f11d69301114e51540
61	0x429a63f16c221da39698144bd56b6d19c6db44f4e40a22eeae2652a7321a28e8
62	0xcf8624aa3b2bd62d8d42185080eade789bb6016de2cd99783bea313dc2744707
63	0xbe3811464bce5070b47c98805a88672ffe38b9a44a69f906f4d227dc287166fe
64	0xafb71cada9337f39c84ea993acce9f552302792563db43db18d8cf93dcdf235f
65	0x1da9561b4a9ff54c9131afc14d8654ab3c7d6f9639f9e4373b442f8f814c98b9
66	0xdc712e195838c1763e9f8a08a27fa0cc3eed8fccaa1bf59a0801ff7db6507381
67	0x6726e3efdedb51a3c7601976ca8f085ee95e364b9174a89fac7edfd2b2da1015
68	0xc237c84cf45ea8122df7f4f9a27d071530c6b58eed1ef75fde505c24980d2cf4
69	0x86acda2bca07925a50928e31c785ba0164e95b6d487d4854b4f8d116c93fe843
70	0x6ad7987a6d10084e2d30f39a885847977187cc6ff23aca8ed0cec7eeaddba143
71	0xd303f10c0748d5df8231287602a8497b188e18053edef36487dde4deb89c76cc
72	0xa9f8704aa1d26ced8dc0abbb1842d83ce1e76f270c068fc86426a01a92386fbc
73	0x484c7f4215c21cd36ba86199c1373e0d6cee9c53cf49224c3f2d8c4f9c8182ea

74	0x6b088a4101e6e38d99175ab6cbddc6bb56f286362e296017bdc1b84d3f1a9b16
75	0x411e150671e68965a7c965816bf57124b2aaa0154cab0e6dd613dd4b080c627b
76	0x2608f6cca0d699fec02743f10435e8d944d976a5b4a53c5f4478704798ced289
77	0x1c09d7202fcbd5aa447dec27a9f872c6405f9dbafc257b449a136be0e0b3cecb
78	0xb0adbb45d85ee0c048169e3dae93b291aeb16a6a5c472ae7fd628a8aaae9d1ef
79	0xf1a67651527010ff7a5c37988a843d7b8f3af2d41c64ef42697f7e20a839d788
80	0x6777f00a1fbb632b58c7548270f1276ef066b25d5861b4747b71798b4e561356
81	0x1de0012fc7dd3e26b73f8cbb62ff1d9b362ea0506ddfab27446b305877e22e59
82	0x997c50b07d6a830bd68b4d85349cd5b8a40d6c58013919db73a6aa40af35a652
83	0xf021141db7c29b4f3d1e81392deeeb5a7dc48c49c02407e8a0bbd9298e9a7944
84	0xf63f709212bf2b6c769f8b6c366dcef671f9ea59fc2d744ef2b3e775b770c2c7
85	0x2d92910a5cda261bc36cc74e9bc9863698facfadfa6c15afd87ff3168dd7f446
86	0xc8f09e160017786f5b1b3ffd758fdcd385870b9b22d31e9d4c2040d3eff23d20
87	0x84c2c1fc445dc005995684d8c6249da28e07523de13800b6c35d248187e6ce4e
88	0xf5500ed7bde2f6a62569f8545bcf3c48aee82176f19e2e7b81015dc46508f1e7
89	0x2cc498426ce75c96511b1d0b52facc892f5859b49a46cd4ad1e9e78163ffed09
90	0xbca9c5a1e7e92c4e79955c4d3cb0339e5e15182f296d00c33fe3df4a66287df2
91	0x2b36a092540d0b927ae9d5302a5e9b504dd5245eddc888b0368c35ea03281bd3
92	0x08a1b4525fd6c0fa92b5e229fbe0bfb15f7ed5780d5054fcea402e5467b30872
93	0x5b77458387dac811b410fe558deac9d28fb5c06c9a114a950d398b2432ccbd40
94	0xa59343c913b14e464883d0b6d28cfe7efdd8d0ba3448ca9e425d7f9e2307f949
95	0xf7ed50b7ae12239a8bee7edc9804b95e3c677d1deaeaeb5c6f3b76976cd512ba
96	0x85e2a9d461d7950e1b853ecc8ee4da536e2c34a69fcd9492e7af1d5960985cbc
97	0x395aaa1a948444f42771f81e24aab115595c4276fdbc78c169448bf6742147dc
98	0xf800319c7226e8942da3d6161ef85435ada754356f085402cb37be4276791ce8
99	0x1f997f1e0e0ee5da9d36f6ed7303121a70d7c648b5379f1928698d9a0a11d578
100	0x24946efaea8dd90e014f280271541c48a9c1d0cdd793aa04c116ced96eec94c6
101	0xed24b47ea1a46bef49d86670d52f69d7db100e0bdec4c07e0bc85f9172ad6d9c
102	0x7a43dae14dc5733564aca43521288276196afc08cede32dcf4af9f20490a7c94
103	0x39fc4792900ce0b4d5a364be72ec167357be8e0cf94ab0bffea8196b4bff5025
104	0x3597b2d6be2602cdc10da881c89b4e823731cf26c62f84b0906577b1065207a7
105	0x5d0e7546c976088b4719ba81011965e6d3b89907ad75b1e6ec367781edbadad8
106	0x5866f339b7c500661fdf467f3517313f6985fce24d98e93923e096efa5acc7e0
107	0x25151b367e2f0ab29c3ac3eacf00a92551b4dce68887b7cfe366a992dac025ea
108	0x24d1b7abadfa8ae497d7e956cb6979873495dbb6f3f291176aa05641556728d7
109	0x27fbfe23710e4eccc17b3b8bcceba06949667ccf27f2c940fb47f619a1e7fa54
110	0x557197c59f4fbdbc6a9e3e870706018c4285a72c21d45a8ab44d950de7ef89d5
111	0xe6067e99901045f4b5a60fccf6a96a835048d2cbb32a9de56719365dcbcda8bd
112	0xfa700adda4a5369a66186339f76ec23598fff2fd7aff8a2685a601c51d5e3fb8
113	0x36e0c0e1bbbb395353b55f37188a6044bf031e210264222704c6585e7dbde24d
114	0x6b948c3c2546fdb1b6f2ddd81730be7185bcb2219a78333a7ed51e85a154dfc6
115	0x35bf32c16ae9d1d05b38d2b5219b6ba0b9e28ebf65ce82544a82b1663aee1b3a
116	0x4e9c177bb4c16a74a6d08db90b93ae5c8226aaf9d102853725bf11835134b50e
117	0xa00f8b8ccd3689f26176f7850461f61a97fae716ea2f6e289273f07394494c79
118	0x253cb54c0cf77973558aedc44021268cbcb711c4d22d16a7a3e3f053be921355

119	0x931e6bdbb41ea6daa93d9a935e4b5050e3bbb7565cde4d4abadcfce5f283d4eb
120	0xcf7bc869b70d4edbfc4ea1733c9be21cdac3e7f780b1472f1365d444e63b4c5a
121	0x7a1cf8daac672977accb2744729fe4eba8d32bea93c7133d4e7d6175a742bb0c
122	0xd0dc2018e4edbc0dbeafeaa2ebc48c2f89d2bca1da9c3db5d79cf4cfa6b17ada
123	0x4263688b28c2bd25013eef25b1075a5571030be81becbd86d0e6043ffd5be68e
124	0x2f0029ef5181ee8699d21a5074543fc72ea5f84411a7458a5366f03870533d21
125	0xcbb5b41f4bc73d90f9135a15000198d3c981c2b9008de7509e033cee180a0529
126	0xbf33a50b94b864b380f37e68478765817baec5b3772356d4a9df301e1c3aa346
127	0xa77db44c77a10a73a726f93995a314a9ba68c5ad20facee0e1ef5343df647e34
128	0xe4599d82ab250b2259eac7d5be430f26acc7576be4991fac60fcde842f8eeb63
129	0x18d993b1db202b1237b311d4acbc199bc02983c548e8908d2222bea87fab4eec
130	0x26f7579350c86964efd53b799494f3b9256560da6d2b6f1523936c21d1642e89
131	0x3a6e1a501a0aad7bdde5242eb1325f48a5d7d37137eb45b0a711ba842f7cba68

XIV. IMPORTANT TERMINOLOGY

6.1 Blockchain

A blockchain is a decentralized and distributed digital ledger or database that is used to record transactions across multiple computers in a secure and transparent manner. Each transaction or record, known as a 'block,' is linked to the previous one through cryptographic hashes, creating a chain of blocks. Once a block is added to the chain, it is difficult to alter, ensuring the integrity of the entire transaction history.

Key characteristics of blockchain include:

- Decentralization: Unlike traditional centralized systems, blockchain operates on a peer-to-peer network, with no single point of control. Each participant in the network (node) has a copy of the entire blockchain.
- Consensus Mechanism: Blockchain relies on a consensus algorithm to validate and agree on the state of the ledger. Common consensus mechanisms include Proof of Work (used in Bitcoin) and Proof of Stake.
- Immutability: Once a block is added to the blockchain, it is cryptographically linked to the previous block, making it extremely difficult to alter. This ensures the integrity of the historical record.
- Transparency: The entire transaction history is visible to all participants in the network. This transparency enhances trust among participants.
- Smart Contracts: Many blockchains support programmable contracts known as smart contracts. These self-executing contracts automatically enforce and execute the terms of an agreement when predefined conditions are met.

6.2 Cryptocurrency

A cryptocurrency is a digital or virtual form of currency that uses cryptography for security and operates on a decentralized network of computers, typically based on blockchain technology. Unlike traditional currencies issued by governments and central banks, cryptocurrencies are decentralized and rely on a technology called blockchain to secure and verify transactions.

6.3 Wallet

A cryptocurrency wallet is a digital tool that allows users to securely store, manage, and interact with their cryptocurrency holdings. Unlike traditional wallets that hold physical currency, a cryptocurrency wallet stores the private and public keys needed to access and manage digital assets on a blockchain.

Key components and features of a cryptocurrency wallet include:

- Public Key: A public key is an address generated by the wallet that serves as the user's receiving address. It can be freely shared with others to receive cryptocurrency payments.
- Private Key: The private key is a secret cryptographic key that is known only to the wallet owner. It is used to sign transactions and gain access to the funds associated with the corresponding public key. Keeping the private key secure is crucial to maintaining control over the cryptocurrency holdings.
- Address: The combination of the public and private keys generates a unique cryptocurrency address for the wallet. This address is used to send and receive digital assets on the blockchain.

- Security: Cryptocurrency wallets employ various security measures to protect private keys and prevent unauthorized access. This may include encryption, password protection, and two-factor authentication.

Types of Wallets:

- Software Wallets: These wallets are software applications that can be installed on computers, smartphones, or other devices. They can be further categorized into desktop wallets, mobile wallets, and web wallets.
- Hardware Wallets: Hardware wallets are physical devices that store private keys offline, providing enhanced security. They are considered more resistant to hacking.
- Paper Wallets: A paper wallet involves printing the public and private keys on a physical document, such as paper. While it is an offline method, it requires careful handling to prevent physical damage or loss.
- Wallet Interoperability: Cryptocurrency wallets are often designed to be compatible with specific cryptocurrencies or multiple cryptocurrencies. Some wallets support a wide range of digital assets, while others are tailored for a particular cryptocurrency.
- Transaction History: Wallets typically provide a transaction history that details the inflow and outflow of cryptocurrency funds. This history is accessible through the wallet's interface.

6.4 Virtual Asset Service Provider (VASP)

A Virtual Asset Service Provider (VASP) is an entity or business that offers services related to virtual assets, including cryptocurrencies and other digital tokens. VASPs play a crucial role in the broader cryptocurrency ecosystem by facilitating the exchange, storage, transfer, and management of virtual assets for users. These services often involve the conversion of virtual assets to fiat currency or other virtual assets.

Key characteristics and functions of Virtual Asset Service Providers include:

- Cryptocurrency Exchanges: VASPs often operate cryptocurrency exchanges, providing platforms where users can buy, sell, and trade various cryptocurrencies. These exchanges serve as intermediaries facilitating the exchange of virtual assets.
- Wallet Providers: VASPs may offer wallet services, allowing users to store, send, and receive virtual assets securely. Wallets can be software-based (online, mobile, or desktop wallets) or hardware-based (physical devices).
- Payment Processors: Some VASPs act as payment processors, enabling merchants to accept virtual assets as a form of payment for goods and services. They facilitate transactions between customers and merchants.
- Token Issuers: Entities that issue and manage digital tokens often fall under the category of VASPs. These tokens may represent various assets, including utility tokens, security tokens, or other digital assets.
- Compliance and Regulation: VASPs are subject to regulatory requirements and must comply with anti-money laundering (AML) and know your customer (KYC) regulations. Compliance helps prevent illicit activities, such as money laundering and terrorist financing, within the virtual asset space.
- Custodial Services: Some VASPs provide custodial services, holding and safeguarding users' private keys and digital assets on their behalf. Custodial services are particularly relevant for institutional investors and users who prefer professional management of their assets.

- Brokerage Services: VASPs may offer brokerage services, allowing users to purchase or sell virtual assets directly through their platforms. Brokers facilitate transactions between buyers and sellers, often providing market liquidity.
- Decentralized Finance (DeFi) Platforms: In the context of decentralized finance, certain DeFi platforms and protocols may be considered VASPs. These platforms enable decentralized lending, borrowing, trading, and other financial services without traditional intermediaries.

6.5 Transaction Hash

A transaction hash is a fundamental element of blockchain technology, providing a unique and tamper-resistant identifier for individual transactions. It plays a crucial role in ensuring the integrity and transparency of blockchain-based systems.

- Uniqueness: Each transaction has a unique transaction hash. Even a small change in the transaction data results in a significantly different hash.
- Verifiability: The transaction hash is crucial for verifying the integrity of transactions on a blockchain. Users can independently calculate the hash of a transaction and compare it with the recorded hash on the blockchain to ensure that the transaction has not been tampered with.
- Blockchain Transparency: Transaction hashes are publicly accessible on the blockchain, providing a transparent and traceable record of all transactions. Users can explore the blockchain using the transaction hash to view details about a specific transaction.
- Linking Blocks: In a blockchain, transaction hashes also play a role in linking blocks together. Each block contains the hash of the previous block (the 'previous hash'), creating a chain of blocks. The hash of a block is influenced by the transactions within it and the previous block's hash.
- Immutability: Because the hash is based on the content of the transaction and is part of the block structure, it contributes to the immutability of transactions on the blockchain. Once a block is added to the blockchain, altering any transaction within it would require changing the hash of that block and all subsequent blocks, which is computationally infeasible.

6.6 Smart Contracts

A smart contract is a self-executing contract with the terms of the agreement directly written into code. It operates on a blockchain, such as Ethereum, and automatically executes and enforces the terms of the contract when predefined conditions are met. Smart contracts aim to automate and facilitate trustless and secure transactions without the need for intermediaries.

Key features and characteristics of smart contracts include:

- Self-Executing: Smart contracts are designed to automatically execute when specific conditions encoded in the contract's code are satisfied. The execution is triggered without the need for external intervention.
- Decentralization: Smart contracts operate on decentralized blockchain networks. Once deployed, they run on a distributed network of nodes, providing transparency, security, and resistance to censorship.
- Code as Contract: The terms and conditions of the contract are expressed in code. This code is stored on the blockchain, making it immutable and tamper-resistant.

- Immutable: Once a smart contract is deployed on the blockchain, its code and terms cannot be altered. This immutability ensures that the contract's execution remains consistent and transparent.
- Trustless: Smart contracts operate in a trustless environment, meaning that participants do not need to trust each other. Trust is established through the code and the decentralized nature of the blockchain.
- Automated Execution: Smart contracts automatically execute predefined actions when specific conditions are met. This automation can include the transfer of digital assets, distribution of funds, or triggering other functions within the contract.
- Cost and Time Efficiency: Smart contracts eliminate the need for intermediaries, reducing costs associated with traditional contract execution. They also operate 24/7 and can execute transactions more quickly than traditional processes.
- Use Cases: Smart contracts find applications in various fields, including finance (decentralized finance or DeFi), supply chain management, voting systems, insurance, gaming, and more.
- Interoperability: Smart contracts can be designed to interact with other smart contracts or decentralized applications (DApps) on the same or different blockchains, enabling interoperability within the broader blockchain ecosystem.

Ethereum is one of the most well-known platforms for deploying and executing smart contracts, but other blockchain platforms also support smart contract functionality. The concept of smart contracts was introduced by Nick Szabo in the 1990s, and their implementation on blockchain technology has significantly expanded their potential use cases.

6.7 Ethereum

Ethereum is an open-source, decentralized blockchain platform that enables the creation and deployment of smart contracts and decentralized applications (DApps). It was proposed by Vitalik Buterin in late 2013 and development started in early 2014, with the network officially launching on July 30, 2015.

Key features and components of Ethereum include:

- Smart Contracts: Ethereum is primarily known for its support of smart contracts, also known as ERC20 tokens, which are self-executing contracts with the terms of the agreement directly written into code. Smart contracts run on the Ethereum Virtual Machine (EVM) and automatically execute when predefined conditions are met.
- Decentralized Applications (DApps): Ethereum provides a platform for the development and deployment of decentralized applications. DApps are applications that run on a peer-to-peer network of computers (nodes) rather than a centralized server.
- Ether (ETH): Ether is the native cryptocurrency of the Ethereum platform. It is used to compensate participants who perform computations (miners) and to pay for transaction fees. Ether can also be used within smart contracts.
- Decentralized Autonomous Organizations (DAOs): Ethereum supports the creation of DAOs, which are organizations governed by smart contracts and run on the Ethereum blockchain. DAOs operate without centralized control and decisions are made by consensus.
- Blockchain Consensus: Ethereum initially used a Proof of Work (PoW) consensus algorithm similar to Bitcoin but is transitioning to Ethereum 2.0, which employs Proof of Stake (PoS) to achieve network security and validate transactions.

- Interoperability: Ethereum has facilitated interoperability through the use of standards such as ERC-20 and ERC-721. ERC-20 defines a common interface for fungible tokens, while ERC-721 is a standard for non-fungible tokens (NFTs), representing unique digital assets.
- Constant Innovation: Ethereum is designed to be a platform for constant innovation. It regularly undergoes upgrades and improvements to enhance scalability, security, and functionality. Ethereum 2.0 is a significant upgrade that aims to address scalability concerns and transition to a more sustainable PoS consensus mechanism.

6.8 The following Ethereum ERC20 Tokens were used in this report:

- Shiba Inu ("SHIB") is a decentralized cryptocurrency created in August 2020 by an anonymous person or group using the pseudonym "Ryoshi". It is inspired by the Shiba Inu, a Japanese dog breed, which also serves as the mascot for Dogecoin, another cryptocurrency with meme origins.
- Hokkaido Inu ("HOKK") is an ERC-20 token that launched on April 17, 2021. HOKK passively rewards for holding through reflections, via a buy and sell tax of 2%/1.77%. •
- Kishu Inu ("KISHU") is a meme token created in the Spring of 2021. The anonymous development team claimed its mission was to bring popular cryptocurrency concepts to the mainstream. So far, it has offered rewards for token holders, a decentralized crypto exchange, and non-fungible tokens (NFTs).
- Akita Inu ("AKITA") is a meme-based cryptocurrency launched on the Ethereum network on February 1, 2021. Inspired by the Akita dog breed, it aligns with other popular meme tokens like Dogecoin and Shiba Inu. Initially introduced as a "social experiment," the project gained attention when 50% of the total supply was sent to Vitalik Buterin's wallet, symbolizing a burn of those tokens.
- FEGtoken ("FEG") is a decentralized crypto project with a singular supply that allows people to buy, trade, bridge between the ETH, BNB and BASE blockchains. The coin was launched in early 2021.
- Hydro (HYDRO) is a decentralized ecosystem that operates on the Ethereum platform. It leverages advanced cryptographic technology to secure user identities, accounts, and transactions. Hydro aims to bring public blockchain technology to traditional private systems, striving to enhance the financial services sector.
- The PAID Network ("PAID"), launched in the second quarter of 2021, is a community-driven decentralized ecosystem that supports blockchain technology to offer "smart agreements" powered by DeFi for making business more efficient.
- DigiCol Token ("DGCL") is focused on digitalizing the collectibles industry. DGCL was intended to revolutionize how digital artists interact with collectors. Their intent was to ensure every digital art piece came with an NFT for digital proof of authentication.

6.9 Tether

Tether (USDT) is a type of cryptocurrency known as a stablecoin, designed to maintain a stable value by pegging it to the value of a fiat currency, usually the US Dollar (USD). Each unit of Tether is intended to be backed by an equivalent amount of traditional currency held in reserves, providing a level of stability and reducing the volatility commonly associated with other cryptocurrencies like Bitcoin or Ethereum.

6.10 TRON

TRON is a blockchain-based platform designed to create a decentralized digital content and entertainment ecosystem. Founded by Justin Sun in 2017, TRON aims to leverage blockchain technology to

build a decentralized internet that allows users to publish, share, and distribute content without the need for traditional intermediaries. TRON's native cryptocurrency is called TRX.

Key features and components of TRON include:

- Blockchain Protocol: TRON operates on its own blockchain protocol, designed to support the creation and execution of smart contracts and decentralized applications (DApps). It uses a delegated proof-of-stake (DPoS) consensus mechanism, allowing a set of elected nodes to validate transactions and produce blocks.
- Smart Contracts: TRON enables the creation and execution of smart contracts, self-executing contracts with the terms written into code. Developers can use the TRON blockchain to deploy and interact with smart contracts, facilitating a variety of decentralized applications.
- Decentralized Applications (DApps): TRON aims to provide a platform for the development and deployment of decentralized applications. These applications can cover a wide range of industries, including gaming, social media, content sharing, and more.
- Content Sharing and Entertainment: One of TRON's primary goals is to revolutionize the digital content and entertainment industry. It seeks to empower content creators by enabling direct transactions between content consumers and producers, reducing the influence of intermediaries.
- TRX Cryptocurrency: TRX is the native cryptocurrency of the TRON blockchain. TRX can be used for various purposes within the TRON ecosystem, including transactions, payments, and as a means of participating in the governance of the network.
- Decentralized Finance (DeFi): TRON has expanded its ecosystem to include decentralized finance (DeFi) applications. These applications offer financial services such as lending, borrowing, and trading on the TRON blockchain.
- Acquisitions and Partnerships: TRON has engaged in strategic partnerships and acquisitions to expand its ecosystem. Notable examples include the acquisition of BitTorrent, a popular peer-to-peer file-sharing platform, and partnerships with various companies in the blockchain and entertainment industries.

6.11 Decentralized Finance (DeFi)

Decentralized Finance (DeFi) refers to a set of financial services and applications built on blockchain technology, particularly on public blockchains like Ethereum. DeFi aims to recreate and innovate traditional financial systems in a decentralized, open, and permissionless manner, allowing individuals to access financial services without relying on traditional banks or financial intermediaries.

Key characteristics of DeFi include:

- Decentralization: DeFi operates on decentralized networks, typically utilizing blockchain technology. This eliminates the need for traditional financial intermediaries, such as banks, and allows users to interact with financial services directly.
- Open Source: DeFi protocols and applications are often open source, meaning that their source code is publicly accessible and can be audited by the community. This transparency contributes to trust and security.
- Interoperability: DeFi projects often aim for interoperability, allowing users to seamlessly use different decentralized applications (DApps) and financial services within the broader DeFi ecosystem.
- Smart Contracts: DeFi relies heavily on smart contracts, which are self-executing contracts with the terms of the agreement directly written into code. Smart contracts automate various financial processes, such as lending, borrowing, and trading.

- Tokenization: DeFi platforms frequently use blockchain-based tokens to represent real-world assets or provide governance within the network. These tokens can represent anything from stablecoins pegged to fiat currencies to unique digital assets.
- Permissionless Access: DeFi services are generally accessible to anyone with an internet connection and a compatible digital wallet. Users can participate without traditional gatekeepers, providing greater financial inclusion.
- Lending and Borrowing: DeFi platforms offer lending and borrowing services where users can lend their assets to earn interest or borrow assets by providing collateral. These processes are often facilitated by smart contracts.
- Decentralized Exchanges (DEXs): DeFi includes decentralized exchanges that allow users to trade digital assets directly from their wallets without the need for a centralized intermediary.
- Automated Market Makers (AMMs): AMMs are a type of decentralized exchange that uses algorithms and liquidity pools to facilitate trades without relying on order books.
- Yield Farming and Liquidity Mining: DeFi platforms often incentivize users to provide liquidity to their protocols by rewarding them with additional tokens. This process, known as yield farming or liquidity mining, encourages active participation.

DeFi has gained significant traction and attention for its potential to transform traditional finance, increase financial accessibility, and introduce new financial instruments. However, users should be aware of potential risks, including smart contract vulnerabilities, market volatility, and regulatory considerations when participating in DeFi activities.

6.12 Decentralized Exchanges (DEX)

A decentralized exchange (DEX) refers to a type of cryptocurrency exchange that operates without a central authority or intermediary. Unlike traditional centralized exchanges where users deposit funds into the exchange's custody, decentralized exchanges allow users to trade directly from their wallets, maintaining control over their private keys and funds throughout the trading process.

Key characteristics of decentralized exchanges include:

- Non-Custodial: DEXs are non-custodial, meaning they do not hold users' funds. Users retain control of their private keys and execute trades directly from their wallets.
- Smart Contracts: DEXs operate on blockchain platforms, such as Ethereum, and utilize smart contracts to automate and facilitate trading processes. Smart contracts act as self-executing agreements that govern the exchange of assets.
- Peer-to-Peer Trading: Trades on decentralized exchanges occur directly between users, creating a peer-to-peer trading environment. Users trade assets without the need for an intermediary.
- Interoperability: DEXs often support a variety of tokens and assets, including those issued on the same blockchain or compatible blockchains. Interoperability allows users to trade a diverse range of digital assets.
- Liquidity Pools: Some decentralized exchanges use liquidity pools, where users can provide liquidity by depositing their assets into a pool. Liquidity providers earn fees for facilitating trades within the pool.
- Permissionless Access: Users can access and trade on decentralized exchanges without the need for a formal registration process. This permissionless access is a key feature of decentralized finance.

- Global Accessibility: DEXs are accessible to users globally, enabling anyone with an internet connection to participate in cryptocurrency trading without geographical restrictions.
- Reduced Counterparty Risk: Since users retain control of their private keys, the risk associated with centralized exchanges, such as hacking or mismanagement of funds, is reduced.
- Popular decentralized exchanges within the DeFi space include Uniswap, SushiSwap, PancakeSwap, and others. These platforms have gained popularity for providing users with more control over their assets, reducing reliance on centralized intermediaries, and fostering a decentralized and open financial ecosystem. However, users should be aware of potential risks, such as smart contract vulnerabilities and market volatility, when participating in decentralized exchanges.

6.13 Bridges

Bridges are mechanisms or protocols that enable the transfer of assets and data between two different blockchain networks. The primary purpose of cryptocurrency bridges is to establish interoperability and connectivity among disparate blockchain ecosystems.

Key points about cryptocurrency bridges include:

- Interoperability: Bridges facilitate communication and interoperability between different blockchain networks that may have distinct protocols, consensus mechanisms, and native assets.
- Asset Transfer: Cryptocurrency bridges allow the transfer of digital assets (such as tokens or cryptocurrencies) from one blockchain to another. This can involve moving assets from a blockchain with one set of features to another blockchain with different features.
- Bi-Directional: Bridges can be bi-directional, meaning they support the transfer of assets in both directions—between the two connected blockchains. This flexibility allows for two-way movement of assets.
- Smart Contracts: Many cryptocurrency bridges utilize smart contracts to lock or escrow assets on one blockchain while creating equivalent assets on the other. Smart contracts play a crucial role in the secure and trustless operation of bridges.
- Cross-Chain Compatibility: Cryptocurrency bridges aim to address the challenge of cross-chain compatibility, enabling seamless interactions between blockchains that use different protocols or standards.
- Decentralization: Some bridges operate in a decentralized manner, leveraging decentralized oracles and smart contracts to facilitate trustless asset transfers. Decentralized bridges aim to reduce reliance on centralized intermediaries.
- Use Cases: Cryptocurrency bridges have various use cases, including facilitating cross-chain asset swaps, enabling cross-chain decentralized finance (DeFi) activities, supporting cross-chain token transfers, and more.
- Security Considerations: Ensuring the security of cryptocurrency bridges is crucial, as they involve the transfer of assets between different blockchains. Implementing robust security measures and conducting thorough audits are essential to mitigate risks.
- Oracle Integration: Some bridges use oracles to obtain external data from one blockchain and provide it to another. Oracles play a role in ensuring that the information needed for cross-chain transactions is accurate.

Cryptocurrency bridges play a vital role in addressing the fragmentation of the blockchain space by enabling seamless communication between different networks. They contribute to the broader goal of creating a more interconnected and interoperable blockchain ecosystem. Developers and users should carefully evaluate the design, security, and functionality of cryptocurrency bridges when considering their use.

6.14 Fiat Money

Fiat money is a type of currency that has no intrinsic value and is not backed by a physical commodity such as gold or silver. Instead, its value is derived from the trust and confidence that people have in the government or authority that issues it. Fiat money is declared legal tender by a government, meaning that it is officially recognized as a medium of exchange for goods and services within a specific jurisdiction.

6.15 Know Your Customer (KYC)

Know Your Customer (KYC) refers to the process by which businesses and financial institutions verify the identity of their customers or users. KYC is a crucial component of regulatory compliance and is designed to prevent illicit activities such as money laundering, terrorism financing, and fraud within the cryptocurrency space.

Key elements of cryptocurrency KYC include:

- Identity Verification: Users are required to provide official identification documents, such as a government-issued ID card, passport, or driver's license, to prove their identity.
- Address Verification: Some KYC processes may include the verification of a user's residential address. This is often done by requesting utility bills, bank statements, or other documents that confirm the user's address.
- Personal Information: Users may be required to provide additional personal information, such as date of birth, nationality, and occupation, to complete the KYC process.
- Source of Funds: In some cases, users may need to disclose the source of the funds they plan to use for cryptocurrency transactions. This helps ensure that the funds are obtained through legal and legitimate means.
- Enhanced Due Diligence (EDD): For certain transactions or high-risk activities, businesses may conduct enhanced due diligence to gather more comprehensive information about the customer.
- Ongoing Monitoring: KYC is not a one-time process. Businesses are required to conduct ongoing monitoring of customer transactions to detect and report any suspicious activities.
- Regulatory Compliance: Cryptocurrency exchanges and other virtual asset service providers are often subject to regulatory requirements related to KYC. Compliance with these regulations is essential to operate legally and maintain a secure and transparent financial environment.

6.16 Greenwich Mean Time (GMT)

Greenwich Mean Time. All times listed in this report have been adjusted for GMT.